Proceedings of the 3rd mini symposium of the Roman Number Theory Association

Università Roma Tre

April 6th, 2017

Contents

Foreword

This volume contains the proceedings of the Third mini symposium of the Roman Number Theory Association. The conference was held on April 6, 2017 at the Università degli Studi Roma Tre. As organizers of the symposium, and promoters of the association, we would like to thank the speakers for the high scientific contribution offered, and the "scribas" who wrote these notes. We also thank the Università Europea di Roma and the Università Roma Tre for funding the event.

The Roman Number Theory Association

The idea of creating this association stems from the desire to bring together Roman researchers who share interest in number theory.

This conference, whose proceedings are collected here, represents the evidence of our goal: to be a key player in the development of a strong Roman community of number theorists, to foster a specific scientific program but also, and more importantly, to create a framework of opportunities for scientific cooperation for anyone interested in number theory. Among these opportunities we can enlist the Scriba project as well as the international cooperation with developing countries and the support of young researcher in number theory with special regards to those coming from developing countries.

The association, even tough founded and based in Rome has an international spirit and we strongly believe in international cooperation.

Our statute is available on the association's website (www.rnta.eu) and it clearly states that our efforts and our funds will be devoted entirely to the development of Number Theory. This will be achieved in several ways: by directly organising events - an annual symposium in Rome as well as seminars distributed over the year; by participating and supporting, both scientifically and financially, workshops, schools and conferences on the topic of interest; by creating a fund to subsidize the participation of young Italian number theorists and mathematicians from developing countries to the activities of the international scientific community.

The Scriba project

The proceedings of a conference usually collect the most significant contributions presented during the conference. The editorial choice, in this case, as for the proceedings of the First and the Second Mini Symposium, was slightly different. In the weeks before the symposium, we identified a list of PhD students and young researchers to whom we proposed to carry out a particular task: that one of the "scriba". Each young scholar was then paired with one of the speakers and was asked to prepare a written report on the talk of the speaker he was assigned to. Of course in doing so the scribas had to get in contact with speakers after the conference in order to get the needed bibliographical references as well as some insight on the topic in question. We would like to highlight that both the speakers and scribas joined the project enthusiastically.

The reasons for this choice lies in the most essential aim of our Association: introducing young researchers to number theory, in all its possible facets. The benefits of this project were twofold: on one hand, the "scribas" had to undertake the challenging task of writing about a topics different from their thesis or their first article subject and learn about a new possible topic of research and, on the other, they had the possibility to collaborate with a senior researcher and learn some trick of the trade.

The manuscripts were approved by the speakers and lastly reviewed by the editors of the present volume.

1 Report on RNTA Activities

In the last four years, the Roman Number Theory Association has been involved in many different activities, here the list of the most significant.

The Fourth mini Symposium of the association will take place on 18-20 April 2018 and, for the first time, have a duration of three days; we will also host, as a satellite conference, the 11th PARI/GP Atelier April 16-17). The annual symposium represents for us a very special moment to bring together most people involved in RNTA and especially our Advisory Board. The proceedings of the first two symposia have been published, and the scriba project is already launched for the fourth one.

Besides, the Association collaborated in various ways to other events, namely:

- *11th Atelier PARI/GP*, Università Roma Tre, to be held in April 16-17, 2018;

- *The Tenth International Conference on Science and Mathematics Education in Developing Countries*, Mandalay University, Myanmar, held in November 2017;

- *Symposium for South Asian Women in Mathematics*, Tribhuvan University (TU), Kathmandu, Nepal, held in October 13th - 15th, 2017;

- *The Ninth International Conference on Science and Mathematics Education in Developing Countries*, Mandalay University, Mandalay, The Republic of the Union of Myanmar, held in November 4-6, 2016;

- *Leuca 2016, Celebrating Michel Waldschmidt's 70th birthday*, Marina di San Gregorio, Patù (Lecce, Italy) held in June 13 - 17, 2016.

Another very important engagement of the association was in the organisation and oparticipation in CIMPA schools. The main idea of CIMPA schools, perfectly matches one of the central aspects of RNTA, namely organising and funding scientific and educational activities in developing countries. The CIMPA schools we are involved in are the following:

- CIMPA research school on *Elliptic curves: arithmetic and computation*. to be held in Universidad de la República, Montevideo, Uruguay, February 11 - 22, 2019.

- CIMPA research school on *Arithmétique algorithmique et cryptographie*. To be held in Université de Kinshasa, Kinshasa, Democratic Republic of Congo, May 7 - 18, 2018.

- CIMPA research school on *Explicit Number Theory*, The Witwatersrand University, Johannesburg, South Africa, January 8 - 19, 2018;

- WAMS research school on *Topics in Analytic and Transcendental Number Theory*, Institute for Advanced Studies in Basic Sciences (IASBS) Zanjan, Iran, July 1 - July 13 2017;

- CIMPA-ICTP research school on *Artin L-functions, Artin's primitive roots conjecture and applications*, Nesin Mathematics Village, Şirince, May 29 - June 9 2017.

- CIMPA-ICTP research school on *Théorie Algébrique des nombres et applications notamment à la cryptographie*, Université Félix Houphouët Boigny, Abidjan, April 10-22, 2017;

- WAMS research school on *Topics in algebraic number theory and Diophantine approximation* , Salahaddin University, Erbil-Kurdistan Region, IRAQ, March 12- 22, 2017;

- CIMPA-ICTP research school on *Lattices and applications to cryptography and coding theory*,Ho Chi Minh University of Pedagogy, August 1 - 12, 2016;

- CIMPA-ICTP research school on *Algebraic curves over finite fields and applications*, University of the Philippines Dillman, July 22 - August 2, 2013.

The Association also supports the *Nepal Algebra Project*. This is a course on Fields and Galois Theory at the Master of Philosophy (M.Phil) and master level (M.Sc.) at Tribhuvan University, Kirtipur, Kathmandu, Nepal.

The project has a span of six years starting with the summer of 2016, ending with the summer of 2021. Each of the six years one course of 50 hours will be offered at Tribhuvan University by several lecturers from developed countries.

Through the past years RNTA collaborated with many institutions, such as

1. International Center for Pure and Applied Mathematics (CIMPA);

2. Istituto Nazionale di Alta Matematica "F. Severi" (INDAM);

3. Abdus Salam International Centre for Theoretical Physics (ICTP);

4. Ministero degli Affari Esteri e della Cooperazione Internazionale (MAECI);

5. Foundation Compositio Mathematica, The Netherlands;

6. Number Theory Foundation (NTF);

7. Centre national de la recherche scientifique (CNRS);

8. International Mathematical Union (IMU);

9. Algebra, Geometry and Number Theory, Erasmus Mundus (ALGANT);

10. Università Roma TRE;

11. Università Europea di Roma.

Marina Monsurrò, Università Europea di Roma
email: marina.monsurro@unier.it

Francesco Pappalardi, Dipartimento di Matematica e Fisica, Università Roma Tre
email: pappa@mat.uniroma3.it

Valerio Talamanca, Dipartimento di Matematica e Fisica, Università Roma Tre
email: valerio@mat.uniroma3.it

Alessandro Zaccagnini, Dipartimento di Scienze Matematiche, Fisiche ed Informatiche, Università di Parma
email: alessandro.zaccagnini@unipr.it

OFFICIAL PHOTO

1. Alejandro Alberto Villa Isaza (*Università Roma Tre*)
2. Louis Nantenaina Andrianaivo (*Università Roma Tre*)
3. Edmond Coleman Koudjinan (*Università Roma Tre*)
4. Guido Maria Lido (*Università di Roma Tor Vergata*)
5. Novak Kaludjerovic (*La Sapienza Università di Roma*)
6. Valerio Dose (*INDAM and Università di Roma Tor Vergata*)
7. Maria Porro (*La Sapienza Università di Roma*)
8. Pietro Mercuri (*La Sapienza Università di Roma*)
9. Fabio Caldarola (*Università della Calabria*)
10. Claudio Fabroni (*Università di Roma Tor Vergata*)
11. Stevan Gajovic (*Serbian Academy of Sciences and Arts*)
12. Carlo Pagano (*Universiteit Leiden*)
13. Frances Odumodu (*Università di Padova and Université de Bordeaux*)
14. Daniele Mastrostefano (*Università di Padova*)
15. Alessandro Gambini (*Università di Parma*)
16. Capi Corrales Rodrigáñez (*Universidad Complutense de Madrid*)
17. Biagio Palumbo (*Università Roma Tre*)
18. Marina Monsurrò (*Università Europea di Roma*)
19. Leonardo Zapponi (*Université Pierre et Marie Curie*)
20. Giacomo Cherubini (*Max-Planck-Institut für Mathematik – Bonn*)
21. Marine Rougnant (*Université de Franche-Comté, Besano̧n*)
22. Remis Tonon (*Università di Parma*)

23. Laura Paladino (*Max-Planck-Institut für Mathematik – Bonn*)
24. Mattia Cafferata (*Università di Parma*)
25. Daniele Cozzo (*La Sapienza Università di Roma*)
26. Francesco Pappalardi (*Università Roma Tre*)
27. Hester Graves (*Institute of Defense Analyses*)
28. René Schoof (*Università di Roma Tor Vergata*)
29. Peter Stevenhagen (*Universiteit Leiden*)
30. Alberto Perelli (*Università di Genova*)
31. Alessandro Zaccagnini (*Università di Parma*)
32. Christian Maire (*Université de Franche-Comté, Besano̧n*)
33. Farshid Hajir (*University of Massachusetts, Amherst*)
34. Lucia Di Vizio (*CNRS - Université de Versailles Saint-Quentine*)
35. Pieter Moree (*Max-Planck-Institut für Mathematik – Bonn*)
36. Fernando Rodriguez Villegas (*International Centre for Theoretical Physics Trieste*)
37. Michel Waldschmidt (*University Pierre et Marie Curie*)
38. Valerio Talamanca (*Università Roma Tre*)

- Mohamed Anwar Mohamed Fouad (*Università Roma Tre*)
- Cristiana Bertolin (*Università di Torino*)
- Nilakantha Paudel (*Università Roma Tre*)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 3, *Number* 1, *March* 2018, *pages* 1-6

Peter Stevenhagen

Primitivity properties of points on elliptic curves

Written by Mattia Cafferata

1 Artin Conjecture

Let $a \in \mathbb{Q}^*$ be a primitive element, i.e. such that $a \neq b^k$ for every integer $k > 1$ and for every $b \in \mathbb{Q}^*$.
Let consider P_a the set the set of prime numbers for which a is a primitive root, $P_a := \{p \text{ prime } : \mathbb{F}_p^* = \langle a \bmod p\rangle\}$, and, assuming that it exists, define $\delta(a)$ as its natural density. One can try to answer the following questions: is the set P_a infinite? When is $\delta(a)$ positive?
Artin, in 1927, made the following conjecture:

Conjecture 1 ***(Artin, 1927)***
Let a be a square-free primitive element of $\mathbb{Q}^*$, then P_a is infinite and

$$\delta(a) = \prod_{q \text{ prime}} \left(1 - \frac{1}{q(q-1)}\right). \tag{1}$$

Artin formulated the conjecture starting from this heuristic argument: he observed that, for almost all p, a prime q divides $\left[\mathbb{F}_p^* : \langle a \bmod p\rangle\right]$ if and only if $p \equiv 1 \; (\bmod\; q)$ and $a \equiv b^q \; (\bmod\; p)$ for some b. The last two conditions, together, are equivalent to ask that the prime p splits completely in the field $L_q := \mathbb{Q}(\zeta_q, a^{1/q})$. So we have that

$$\mathbb{F}_p^* = \langle a \bmod p \rangle \iff \text{for no prime } q, p \text{ splits completely in } L_q.$$

By the Chebotarev Density Theorem, the density of primes which split completely in L_q equals, generically,

$$\frac{1}{[L_q : \mathbb{Q}]} = \frac{1}{q(q-1)}$$

one can expect (1) to be valid.

It's interesting to observe that the right-hand side of (1) does not depend from a and so it's reasonable to think that the formula may need some correction to hold for every "primitive" element in $\mathbb{Q}^*$. In fact, the events "p splits completely in L_{q_1}" and "p splits completely in L_{q_2}" are not not necessarily independent as q_1 and q_2 range through all primes. For example, if $a = 5$, then

$$L_2 = \mathbb{Q}(\sqrt{5}) \subset \mathbb{Q}(\zeta_5, 5^{1/5}) = L_5.$$

A more general form of the conjecture was given by Lehmer and Artin himself in 1953 and later in 1967 Hooley proved the following theorem:

Theorem 1 *Let $a \in \mathbb{Q}^*$ a primitive element; then, under GRH, we have*

$$\delta(a) = \sum_{k=1}^{\infty} \frac{\mu(k)}{[L_k : \mathbb{Q}]} \tag{2}$$

where μ is the Möbius function.

The the Möbius function solves the entanglement problem, i.e. the fact that the field L_q are not always linearly disjoint over $\mathbb{Q}$.

2 Lang-Trotter Conjecture

Artin's problem is pertinent to many generalizations and variations. A natural generalization appears in the context of elliptic curves and was formulated by S. Lang and H. Trotter in 1976.
Let E be an elliptic curve defined over $\mathbb{Q}$ and let $A \in E(\mathbb{Q})$ be a primitive point, i.e. such that $A \neq kB$ for every integer $k > 1$ and for every $B \in E(\mathbb{Q})$. For a prime p of good reduction for E, let $E(\mathbb{F}_p)$ be the reduction of $E(\mathbb{Q})$ modulo p.

Conjecture 2 ***(Lang, Trotter, 1976)*** *For every elliptic curve $E(\mathbb{Q})$ and every primitive $A \in E(\mathbb{Q})$ the set*

$$\{p \; prime \; : E(\mathbb{F}_p) = \langle A \mod p \rangle\}$$

has natural density $\delta_E(A) \geq 0$.

An important remark is that, in contrast with the classical situation, when we require that $E(\mathbb{F}_p) = \langle A \mod p\rangle$ we are making the implicit assumption that $E(\mathbb{F}_p)$ is cyclic.

In general, $E(\mathbb{F}_p)$ is the product of two cyclic groups, therefore it is natural to consider, at first, the question of finding the density of primes p for which $E(\mathbb{F}_p)$ is cyclic. Again we can use an heuristic approach: denote by $E[m]$ the set of m-torsion points and with $Z_q = \mathbb{Q}(E[q])$ the q-division field. It can be showed that

$$\begin{aligned} E(\mathbb{F}_p) \text{ is cyclic } &\iff \text{ for no prime } q, \quad E[q](\mathbb{F}_p) \neq q^2 \\ &\iff p \text{ does not split completely in any field } Z_q. \end{aligned}$$

This leads to a conjecture similar to the one in (2), which was conditionally proved by Serre

Theorem 2 ***(Serre, 1993)*** *Let $E/\mathbb{Q}$ be an elliptic curve. Then, under GRH, the density δ_E of the set $\{p \; prime : E(\mathbb{F}_p) \text{ is cyclic}\}$ exists and*

$$\delta_E = \sum_{k=1}^{\infty} \frac{\mu(k)}{[Z_k : \mathbb{Q}]} \tag{3}$$

An unconditional in the direction of the above conjecture was given by M.R Murty in 1988 for elliptic curves with complex multiplication.

3 Primitivity on elliptic curves

Very little is known about the density $\delta_E(A)$ and the results obtained so far require at least to assume *GRH* and additional hypothesis on the elliptic curve.
To better understand the difference between the classical and the elliptic curve case we can analyse the problem from another point of view. We begin with the classical case.
Consider V_q the 2-dimensional vector space over $\mathbb{F}_q$ defined by

$$V_q = \langle \zeta_q, a^{1/q} \rangle / \langle a \rangle.$$

We can define an action of $G_q = \mathrm{Gal}(L_q/\mathbb{Q})$ over V_q identifying the elements of G_q with the matrices

$$\left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a \in \mathbb{F}_q^*, b \in \mathbb{F}_q \right\} \subset \mathrm{Aut}(V_q).$$

So, if we denote with $\phi_p \in G$ the Frobenius map we get that, for almost all p

$$\begin{aligned} q \text{ divides } \left[\mathbb{F}_p^* : \langle a \bmod p \rangle\right] &\iff \phi_p \text{ acts trivially on } V_q \\ &\iff V_q^{\langle \phi_p \rangle} = V_q \end{aligned}$$

In the elliptic case, instead, we consider the 3-dimensional space V_p defined as

$$V_q = \langle E[q], q^{-1}A \rangle / \langle A \rangle.$$

Analogously to the previous case we define an action $G_q = \mathrm{Gal}(Z_q/\mathbb{Q})$ over V_q identifying the elements of G_q with the matrices

$$\left\{ \left(\begin{array}{cc|c} \multicolumn{2}{c|}{\multirow{2}{*}{B}} & a \\ & & b \\ \hline 0 & 0 & 1 \end{array} \right) : a, b \in \mathbb{F}_q, B \in GL_2(\mathbb{F}_q) \right\} \subset \mathrm{Aut}(V_q).$$

In this case it can be proved that for almost all p

$$q \text{ divides } \left[E(\mathbb{F}_p) : \langle A \bmod p\rangle\right] \iff \dim(V_q^{\langle \phi_p \rangle}) \geq 2.$$

We note that, in the second situation, the condition $V_q^{\langle \phi_p \rangle} = V_q$ is sufficient, but non more necessary to expect non primitivity.
For a generic point of an elliptic curve we can say what follows:

Theorem 3 *Let $E(\mathbb{Q})$ be an elliptic curve and A any point of $E(\mathbb{Q})$; then q divides $\left[E(\mathbb{F}_p) = \langle A \mod p\rangle\}\right]$ for almost all primes p if and only if one of the following holds:*

1. *$E[q](\mathbb{Q}) = q^2$;*

2. *q divides $|E(\mathbb{Q})^{tor}|$ and $A = qB \in E(\mathbb{Q})$;*

3. *exists $\varphi_{|\mathbb{Q}} : E(\mathbb{Q}) \to E'(\mathbb{Q})$ of degree q such that condition (2) holds for $E'(\mathbb{Q})$ and $\varphi(A)$.*

Finally we recall a result by G. Meleleo who showed, in his Ph.D. thesis that is possible to have a never-primitivity situation;

Theorem 4 ***(Meleleo,2015)***
There exists elliptic curves $E(\mathbb{Q})$ with primitive points $A \in E(\mathbb{Q})$ such that $E(\mathbb{F}_p) \neq \langle A \mod p\rangle$ for almost all primes p.

References

[1] C. Hooley, *On Artin's conjecture*, J. Reine Angew. Math.,1967

[2] S. Lang, H. Trotter, *Primitive points on elliptic curves*, Bull. Amer. Math. Soc., 1977.

[3] G. Meleleo, *Questions related to primitive points on elliptic curves and statistics for biquadratic curves over finite fields*, Ph.D. Thesis, 2015.

[4] P. Moree, *Artin's Primitive Root Conjecture - A Survey*, 2012.

[5] M. R. Murty, *Artin's conjecture for primitive roots*, Math. Intelligencer 10, 1988.

Mattia Cafferata
Dipartimento di Scienze Matematiche, Fisiche e Informatiche
Università di Parma
parco Area delle scienze 53/a
43124 Parma, italy.
email: `mattia.cafferata@unife.it`

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 3, *Number* 1, *March* 2018, *pages* 13-23

Michel Waldschmidt

Diophantine approximations and continued fractions

written by Stevan Gajović

Introduction

In the introduction of his paper in 1873, where he proved the transcendence of e, Ch. Hermite starts by recalling the theory of simultaneous Diophantine approximation to several real numbers by rational tuples. He points out that the case of a single number is nothing else than the algorithm of continued fractions. He claims that he will do something similar with functions. This is the birth of the theory of Padé approximation, and Hermite pursues by giving an explicit solution for what is now called Padé approximants of type II for the exponential function.

Rational approximations to a real number

We start with one simple fact. If x is a rational number, there is a constant $c > 0$ such that for any $\frac{p}{q} \in \mathbb{Q}$ with $\frac{p}{q} \neq x$, we have $|x - \frac{p}{q}| \geq \frac{c}{q}$. This statement can easily be proven, we just need to write x as $x = \frac{a}{b}$ and set $c = \frac{1}{b}$.

On the other hand, if x is a real irrational number, there are infinitely many $\frac{p}{q} \in \mathbb{Q}$, with $\gcd(p, q) = 1$ such that $|x - \frac{p}{q}| < \frac{1}{q^2}$. This is a conwhere a variable T represents $Z_{n-1} + \frac{1}{Z_n}$. Then, the proof follows by using inductive hypothesis (twice), replacement $T = Z_{n-1} + \frac{1}{Z_n}$ and simple calculations.

The matrix form is

$$\begin{pmatrix} P_n \\ Q_n \end{pmatrix} = \begin{pmatrix} P_{n-1} & P_{n-2} \\ Q_{n-1} & Q_{n-2} \end{pmatrix} \begin{pmatrix} Z_n \\ 1 \end{pmatrix}.$$

It is a better idea to consider 2 × 2 matrices

$$\begin{pmatrix} P_n & P_{n-1} \\ Q_n & Q_{n-1} \end{pmatrix} = \begin{pmatrix} P_{n-1} & P_{n-2} \\ Q_{n-1} & Q_{n-2} \end{pmatrix} \begin{pmatrix} Z_n & 1 \\ 1 & 0 \end{pmatrix}.$$

Hence, there is a nice formula for the polynomials P_n and Q_n

$$\begin{pmatrix} P_n & P_{n-1} \\ Q_n & Q_{n-1} \end{pmatrix} = \begin{pmatrix} Z_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} Z_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} Z_n & 1 \\ 1 & 0 \end{pmatrix} \quad \text{for } n \geq -1,$$

if we define

$$\begin{pmatrix} P_{-1} & P_{-2} \\ Q_{-1} & Q_{-2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

and treat an empty product (the case $n = -1$) as the identity matrix.

There are a few definitions we will need to work with continued fractions. Let $x = [a_0,\ a_1,\ a_2, \ldots, a_n]$. As we have seen, $x = \frac{p_n}{q_n}$, with $p_n = P_n(a_0, a_1, \ldots, a_n)$ and $q_n = Q_n(a_1, \ldots, a_n)$. For $x = [a_0,\ a_1,\ a_2, \ldots, a_n, \ldots]$, the rational numbers in the sequence

$$\frac{p_n}{q_n} = [a_0,\ a_1,\ a_2, \ldots, a_n] \qquad (n = 1, 2, \ldots)$$

give rational approximations for x which are the best ones when comparing the quality of the approximation and the size of the denominator. We call $a_0, a_1, a_2, \ldots$ the *p*artial quotients. Additionally, $\frac{p_n}{q_n}$ $(n \geq 0)$ are for $i \geq 1$.

For $x \in \mathbb{F}((1/T))$, we have the same definitions as before. Let

$$x = [A_0, A_1, \dots]$$

be a continued fraction. Then polynomials A_n are called *p*artial quotients , rational functions $\frac{P_n}{Q_n}$, with $P_n = P_n(A_0, A_1, \dots, A_n)$ and $Q_n = Q_n(A_1, \dots, A_n)$ are called *c*onvergents and members of the sequence $x_n = [A_n, A_{n+1}, \dots]$ are *c*omplete quotients.

Also, it is true that

$$x = [A_0, A_1, \dots, A_{n-1}, x_n] = \frac{x_n P_{n-1} + P_{n-2}}{x_n Q_{n-1} + Q_{n-2}}.$$

For $x = [A_0, A_1, \dots] \in \mathbb{F}((1/T))$,

$$P_n = P_n(A_0, A_1, \dots, A_n), \quad Q_n = Q_n(A_1, \dots, A_n),$$

one can prove that

$$|Q_n| = |A_n| \cdot |A_{n-1}| \cdots |A_1| \quad (n \geq 1)$$

and

$$\left| x - \frac{P_n}{Q_n} \right| = \frac{1}{|Q_n|\,|Q_{n+1}|} = \frac{1}{|A_{n+1}|\,|Q_n|^2} \quad (n \geq 0).$$

In this case it is also true that the convergents are the best rational approximations, namely the following is true.

Theorem 2. *Let $\frac{P_n}{Q_n}$ be the n–th convergent of the continued fraction expansion of $x \in \mathbb{F}((T^{-1})) \smallsetminus \mathbb{F}(T)$. Let $\frac{A}{B}$ be any element in $\mathbb{F}(T)$ such that $|B| \leq |Q_n|$. Then*

$$|Q_n x - P_n| \leq |Bx - A|$$

with equality if and only if $(A, B) = (P_n, Q_n)$.

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 3, *Number* 1, *March* 2018, *pages* 13-23

Michel Waldschmidt

Diophantine approximations and continued fractions

written by Stevan Gajović

Introduction

In the introduction of his paper in 1873, where he proved the transcendence of e, Ch. Hermite starts by recalling the theory of simultaneous Diophantine approximation to several real numbers by rational tuples. He points out that the case of a single number is nothing else than the algorithm of continued fractions. He claims that he will do something similar with functions. This is the birth of the theory of Padé approximation, and Hermite pursues by giving an explicit solution for what is now called Padé approximants of type II for the exponential function.

Rational approximations to a real number

We start with one simple fact. If x is a rational number, there is a constant $c > 0$ such that for any $\frac{p}{q} \in \mathbb{Q}$ with $\frac{p}{q} \neq x$, we have $|x - \frac{p}{q}| \geq \frac{c}{q}$. This statement can easily be proven, we just need to write x as $x = \frac{a}{b}$ and set $c = \frac{1}{b}$.

On the other hand, if x is a real irrational number, there are infinitely many $\frac{p}{q} \in \mathbb{Q}$, with $\gcd(p, q) = 1$ such that $|x - \frac{p}{q}| < \frac{1}{q^2}$. This is a consequence of the Dirichlet's theorem, which states that for any positive real number α and any positive integer N, there exist coprime integers p and q such that $1 \leq q \leq N$ and $|q\alpha - p| \leq \dfrac{1}{N}$.

It is known that the best rational approximations $\frac{p}{q}$ are given by the algorithm of continued fractions. We will give a short survey on this algorithm.

Before doing so, we give two generalisations of the problem in higher dimension. Let $x_1, \dots, x_m$ be given real numbers, we may either consider

$$\max_{1 \leq i \leq m} \left| x_i - \frac{p_i}{q} \right|,$$

for $p_1, \dots, p_m, q$ in $\mathbb{Z}$ with $q > 0$, which is the simultaneous approximation of the tuple $(x_1, \dots, x_m)$ by rational numbers with the same denominator, or else

$$|p_1 x_1 + \dots + p_m x_m - q|$$

$p_1, \dots, p_m, q$ in $\mathbb{Z}$ not all zero.

As we want to give analogues for power series, let us note that the first one corresponds to Padé approximants of type II and the second one corresponds to Padé approximants of type I.

The continued fractions

We explain very briefly the algorithm of continued fractions. Let $x \in \mathbb{R}$. Imitating Euclidean division, we can "divide" x by 1

$$x = \lfloor x \rfloor + \{x\},$$

with $\lfloor x \rfloor \in \mathbb{Z}$ and $0 \leq \{x\} < 1$. If x is not an integer, then $\{x\} \neq 0$. Set $x_1 = \frac{1}{\{x\}}$, so that

$$x = \lfloor x \rfloor + \frac{1}{x_1},$$

and $x_1 > 1$. If x_1 is not an integer, set $x_2 = \frac{1}{\{x_1\}}$ and write

$$x = \lfloor x \rfloor + \frac{1}{\lfloor x_1 \rfloor + \{x_1\}} = \lfloor x \rfloor + \frac{1}{\lfloor x_1 \rfloor + \frac{1}{x_2}}$$

with $x_2 > 1$. Set $a_0 = \lfloor x \rfloor$ and $a_i = \lfloor x_i \rfloor$ for $i \geq 1$. Then

$$x = \lfloor x \rfloor + \cfrac{1}{[x_1] + \cfrac{1}{\lfloor x_2 \rfloor + \cfrac{1}{\ddots}}} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}}$$

So, we can see the explanation of the name continued fraction. We use the notation $x = [a_0,\ a_1,\ a_2,\ a_3, \dots]$. As a matter of fact, the algorithm stops after finitely many steps if and only if x is rational.

If x is rational, we can recognize the Euclidean division. Write $x = \frac{p}{q}$, then divide p by q: $p = a_0 q + r_0$, where $0 \leq r_0 < q$. If $r_0 \neq 0$, then consider $x_1 = \frac{q}{r_0} > 1$ and do the same: $q = a_1 r_0 + r_1$, $0 \leq r_1 < r_0$, then $r_1 = 0$ or put $x_2 = \frac{r_0}{r_1}$ etc. Since Euclidean algorithm stops, this one will too, which confirms our claim on finite continued fraction of a rational number.

Let $a_0, a_1, \dots, a_n$ be given integers with $a_i \geq 1$ for $i \geq 1$. Then the finite continued fraction $[a_0,\ a_1,\ a_2,\ a_3, \dots, a_n]$ can be written as

$$\frac{P_n(a_0, a_1, \dots, a_n)}{Q_n(a_1, a_2, \dots, a_n)},$$

where P_n and Q_n are polynomials with integer coefficients. We would like to write these polynomials explicitly.

Let $\mathbb{F}$ be a field, $Z_0, Z_1, \dots$ variables. We will define polynomials P_n and Q_n in $\mathbb{F}[Z_0, \dots, Z_n]$ and $\mathbb{F}[Z_1, \dots, Z_n]$ respectively such that

$$[Z_0, Z_1, \dots, Z_n] = \frac{P_n}{Q_n}.$$

Here are the first values:

$$P_0 = Z_0, \quad Q_0 = 1, \quad \frac{P_0}{Q_0} = Z_0;$$

$$P_1 = Z_0 Z_1 + 1, \quad Q_1 = Z_1, \quad \frac{P_1}{Q_1} = Z_0 + \frac{1}{Z_1};$$

$$P_2 = Z_0 Z_1 Z_2 + Z_2 + Z_0, \quad Q_2 = Z_1 Z_2 + 1, \quad \frac{P_2}{Q_2} = Z_0 + \frac{1}{Z_1 + \frac{1}{Z_2}}$$

$$P_3 = Z_0 Z_1 Z_2 Z_3 + Z_2 Z_3 + Z_0 Z_3 + Z_0 Z_1 + 1, \quad Q_3 = Z_1 Z_2 Z_3 + Z_3 + Z_1,$$

$$\frac{P_3}{Q_3} = Z_0 + \frac{1}{Z_1 + \frac{1}{Z_2 + \frac{1}{Z_3}}}.$$

We can easily observe the relations between these polynomials:

$$P_2 = Z_2 P_1 + P_0, \quad Q_2 = Z_2 Q_1 + Q_0.$$

$$P_3 = Z_3 P_2 + P_1, \quad Q_3 = Z_3 Q_2 + Q_1.$$

We infer that a more general rule holds. Let us define two sequences of polynomials in the following way:

$$P_n = Z_n P_{n-1} + P_{n-2}, \quad Q_n = Z_n Q_{n-1} + Q_{n-2}.$$

One can check that it is really true that $[Z_0, Z_1, \ldots, Z_n] = \dfrac{P_n}{Q_n}$ for all $n \geq 0$. Indeed, we can prove this by induction. As we saw, the statement is true for small numbers $n = 1, 2, 3$. To show the inductive step, we need to write

$$[Z_0, Z_1, \ldots, Z_n] = \frac{P_{n-1}(Z_0, \ldots, Z_{n-2}, T)}{Q_{n-1}(Z_1, \ldots, Z_{n-2}, T)},$$

where a variable T represents $Z_{n-1} + \frac{1}{Z_n}$. Then, the proof follows by using inductive hypothesis (twice), replacement $T = Z_{n-1} + \frac{1}{Z_n}$ and simple calculations.

The matrix form is

$$\begin{pmatrix} P_n \\ Q_n \end{pmatrix} = \begin{pmatrix} P_{n-1} & P_{n-2} \\ Q_{n-1} & Q_{n-2} \end{pmatrix} \begin{pmatrix} Z_n \\ 1 \end{pmatrix}.$$

It is a better idea to consider 2 × 2 matrices

$$\begin{pmatrix} P_n & P_{n-1} \\ Q_n & Q_{n-1} \end{pmatrix} = \begin{pmatrix} P_{n-1} & P_{n-2} \\ Q_{n-1} & Q_{n-2} \end{pmatrix} \begin{pmatrix} Z_n & 1 \\ 1 & 0 \end{pmatrix}.$$

Hence, there is a nice formula for the polynomials P_n and Q_n

$$\begin{pmatrix} P_n & P_{n-1} \\ Q_n & Q_{n-1} \end{pmatrix} = \begin{pmatrix} Z_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} Z_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} Z_n & 1 \\ 1 & 0 \end{pmatrix} \qquad \text{for } n \geq -1,$$

if we define

$$\begin{pmatrix} P_{-1} & P_{-2} \\ Q_{-1} & Q_{-2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

and treat an empty product (the case $n = -1$) as the identity matrix.

There are a few definitions we will need to work with continued fractions. Let $x = [a_0,\ a_1,\ a_2, \ldots, a_n]$. As we have seen, $x = \frac{p_n}{q_n}$, with $p_n = P_n(a_0, a_1, \ldots, a_n)$ and $q_n = Q_n(a_1, \ldots, a_n)$. For $x = [a_0,\ a_1,\ a_2, \ldots, a_n, \ldots]$, the rational numbers in the sequence

$$\frac{p_n}{q_n} = [a_0,\ a_1,\ a_2, \ldots, a_n] \qquad (n = 1, 2, \ldots)$$

give rational approximations for x which are the best ones when comparing the quality of the approximation and the size of the denominator. We call $a_0, a_1, a_2, \ldots$ the *p*artial quotients. Additionally, $\frac{p_n}{q_n}$ $(n \geq 0)$ are the convergents, whereas $x_n = [a_n, a_{n+1}, \dots]$ ($n \geq 0$) are the complete quotients. Also, note

$$x = [a_0, a_1, \dots, a_{n-1}, x_n] = \frac{x_n p_{n-1} + p_{n-2}}{x_n q_{n-1} + q_{n-2}}.$$

There are some inequalities that are worth mentioning, such as

$$a_n q_{n-1} \leq q_n \leq (a_n + 1) q_{n-1}$$

and

$$\frac{1}{(a_{n+1}+2)q_n} < \frac{1}{q_{n+1}+q_n} < |q_n x - p_n| < \frac{1}{q_{n+1}} < \frac{1}{a_{n+1}q_n}.$$

The most important property of convergents is that they are the best rational approximations (in a size of a denominator). Indeed, we have the following theorem and an easy consequence.

Theorem 1. *Let $\frac{p_n}{q_n}$ be the n–th convergent of the continued fraction expansion of an irrational number x. Let $\frac{a}{b}$ be any rational number, such that $1 \leq b \leq q_n$. Then*

$$|q_n x - p_n| \leq |bx - a|,$$

with equality if and only if $(a, b) = (p_n, q_n)$.

Corollary 1.1. *For $1 \leq b \leq q_n$ we have*

$$\left| x - \frac{p_n}{q_n} \right| \leq \left| x - \frac{a}{b} \right|,$$

with equality if and only if $(a, b) = (p_n, q_n)$.

Analogies in the power series case

Let us now describe the analogy with power series. Let $\mathbb{F}$ be a field. For $\dfrac{P}{Q} \in \mathbb{F}(T)$, define

$$\left|\frac{P}{Q}\right| = e^{\deg P - \deg Q}$$

with $|0| = 0$. We can easily check that this function satisfies all of the properties of absolute value on the field $\mathbb{F}(T)$: positive-definiteness, multiplicativity, the triangle inequality. The field $\mathbb{F}(T)$ is not complete with respect to this absolute value, and its completion is $\mathbb{F}((1/T))$. The absolute value is extended in the following way - for $x \in \mathbb{F}((1/T))$ with $x \neq 0$ and

$$x = a_{k_0}T^{k_0} + a_{k_0-1}T^{k_0-1} + \cdots = \sum_{k \le k_0} a_k T^k$$

where $k_0 \in \mathbb{Z}$, $a_k \in \mathbb{F}$ for all $k \le k_0$ and $a_{k_0} \neq 0$, we define $|x| = e^{k_0}$.

Here we can see the analogues between the real numbers and the power series case:

$$\begin{tikzcd}
\mathbb{Z} \arrow[r, phantom, "\subset"] \arrow[d, leftrightarrow] & \mathbb{Q} \arrow[r, phantom, "\subset"] \arrow[d, leftrightarrow] & \mathbb{R} \arrow[d, leftrightarrow] \\
\mathbb{F}[T] \arrow[r, phantom, "\subset"] & \mathbb{F}(T) \arrow[r, phantom, "\subset"] & \mathbb{F}((1/T))
\end{tikzcd}$$

$$\mathbb{Q} : \text{norm} \quad \left|\frac{a}{b}\right| = \max\{|a|, |b|\}, \quad \text{completion} \quad \sum_{n \ge -k} a_n 10^{-n} \longrightarrow \mathbb{R},$$

$$\mathbb{F}(T) : \text{norm} \quad \left|\frac{P}{Q}\right| = e^{\deg P - \deg Q}, \quad \text{completion} \quad \sum_{n \ge -k} a_n T^{-n} \longrightarrow \mathbb{F}((1/T)).$$

Notice that any element in $\mathbb{F}(T)$ has a unique continued fraction expansion $[A_0, A_1, \ldots, A_n]$ with $A_i \in \mathbb{F}[T]$ for $i \ge 0$ and $\deg A_i \ge 1$

for $i \geq 1$.

For $x \in \mathbb{F}((1/T))$, we have the same definitions as before. Let

$$x = [A_0, A_1, \dots]$$

be a continued fraction. Then polynomials A_n are called *p*artial quotients , rational functions $\frac{P_n}{Q_n}$, with $P_n = P_n(A_0, A_1, \dots, A_n)$ and $Q_n = Q_n(A_1, \dots, A_n)$ are called *c*onvergents and members of the sequence $x_n = [A_n, A_{n+1}, \dots]$ are *c*omplete quotients.

Also, it is true that

$$x = [A_0, A_1, \dots, A_{n-1}, x_n] = \frac{x_n P_{n-1} + P_{n-2}}{x_n Q_{n-1} + Q_{n-2}}.$$

For $x = [A_0, A_1, \dots] \in \mathbb{F}((1/T))$,

$$P_n = P_n(A_0, A_1, \dots, A_n), \quad Q_n = Q_n(A_1, \dots, A_n),$$

one can prove that

$$|Q_n| = |A_n| \cdot |A_{n-1}| \cdots |A_1| \quad (n \geq 1)$$

and

$$\left| x - \frac{P_n}{Q_n} \right| = \frac{1}{|Q_n|\,|Q_{n+1}|} = \frac{1}{|A_{n+1}|\,|Q_n|^2} \quad (n \geq 0).$$

In this case it is also true that the convergents are the best rational approximations, namely the following is true.

Theorem 2. *Let $\frac{P_n}{Q_n}$ be the n–th convergent of the continued fraction expansion of $x \in \mathbb{F}((T^{-1})) \setminus \mathbb{F}(T)$. Let $\frac{A}{B}$ be any element in $\mathbb{F}(T)$ such that $|B| \leq |Q_n|$. Then*

$$|Q_n x - P_n| \leq |Bx - A|$$

with equality if and only if $(A, B) = (P_n, Q_n)$.

There is a straightforward corollary.

Corollary 2.1. *For $|B| \le |Q_n|$ we have*

$$\left|x - \frac{P_n}{Q_n}\right| \le \left|x - \frac{A}{B}\right|$$

with equality if and only if $(A, B) = (P_n, Q_n)$.

Let us state a few theorems in the case of real numbers and function fields.

Theorem 3. *(Legendre Theorem)*
(1) ***R****eal numbers: If $x \in \mathbb{R} \setminus \mathbb{Q}$ and*

$$\left|x - \frac{p}{q}\right| < \frac{1}{2q^2},$$

then $\frac{p}{q}$ is a convergent of x.
(2) ***P****ower series: If $x \in \mathbb{F}((T^{-1})) \setminus \mathbb{F}(T)$ and*

$$\left|x - \frac{P}{Q}\right| < \frac{1}{|Q|^2},$$

then $\frac{P}{Q}$ is a convergent of x.

Theorem 4. *(Lagrange Theorem)*
(1) ***R****eal numbers: The continued fraction expansion of a real irrational number x is ultimately periodic if and only if x is quadratic over $\mathbb{Q}$.*
(2) ***P****ower series: If the continued fraction expansion of an element $x \in \mathbb{F}((T^{-1})) \setminus \mathbb{F}(T)$ is ultimately periodic, then x is quadratic over $\mathbb{F}(T)$. The converse is true when the field has nonzero characteristic and is an algebraic extension of its prime field $\mathbb{F}_p$ (but not otherwise).*

Let us recall that ultimately periodic sequence is a sequence that is periodic starting from some index. An element $x \in \mathbb{F}((T^{-1})) \setminus \mathbb{F}(T)$ has a *pseudo periodic expansion*, namely an expansion of the form

$$[A_0, A_1, \dots, A_{n-1}, B_1, \dots, B_{2t}, aB_1, a^{-1}B_2, aB_3, \dots, a^{-1}B_{2t},$$

$$a^2B_1, a^{-2}B_2, \ldots, a^{-2}B_{2t}, a^3B_1, a^{-3}B_2, \ldots],$$

if and only if there exist R, S, T, U in $\mathbb{F}[T]$ with

$$x = \frac{Rx + S}{Tx + U}$$

where $\begin{pmatrix} R & S \\ T & U \end{pmatrix}$ has determinant 1 and is not a multiple of the identity matrix.
If D is polynomial which is irreducible over any quadratic extension of $\mathbb{F}$ then the regular continued fraction expansion of $\sqrt{D}$ is not pseudo–periodic.

We conclude by mentioning that there is a formal analogy between Nevanlinna theory and Diophantine approximation. Via Vojta's dictionary, the Second Main Theorem in Nevanlinna theory corresponds to Schmidt's Subspace Theorem in Diophantine approximation.

References

[1] P. Flajolet, B. Vallée, I. Vardi, *Continued fractions from Euclid to the present day*, 44p. `http://www.lix.polytechnique.fr/Labo/Ilan.Vardi/continued_fractions.ps`

[2] A. Lasjaunias, *A survey of Diophantine approximation in fields of power series*. *Monatsh. Math.*, 130(3):211–229, 2000.

[3] A. Lasjaunias, *Diophantine approximation and continued fractions in power series fields*. `https://www.math.u-bordeaux.fr/~alasjaun/survey.pdf`

[4] W. M. Schmidt, *On continued fractions and Diophantine approximation in power series fields*. Acta Arith., 95(2):139–166, 2000.

Stevan Gajović
University of Belgrade
Faculty of Mathematics, Department of Algebra
Studentski trg 16
11000 Belgrade, Serbia.
email: stevangajovic@gmail.com

current address:
University of Groningen
Nijenborgh 9
9747 AG Groningen, The Netherlands

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 3, *Number* 1, *March* 2018, *pages* 25-29

Alberto Perelli

A Rigidity theorem for translates of uniformly convergent Dirichlet series

Written by Daniele Mastrostefano

In 1975, Voronin [6] discovered the following universality property of the Riemann zeta function $\zeta(s)$: given an holomorphic and non-vanishing function $f(s)$ on a closed disk K inside the critical strip $\frac{1}{2} < \sigma < 1$, for every $\varepsilon > 0$, we have

$$\liminf_{T\to\infty} \frac{1}{2T} |\{\tau \in [-T, T] : \max_{s\in K} |\zeta(s + i\tau) - f(s)| < \varepsilon\}| > 0. \qquad (1)$$

Voronin's universality theorem has been extended in several directions, in particular involving other L-functions in place of $\zeta(s)$ or vector of L-functions in place of a single L-function and other compact sets in place of disks; see the survey by Matsumoto [**?**] and Chapter VII of Karatsuba-Voronin [2]. Those results cannot yet be valid in the region $\sigma > 1$, since every Dirichlet series $F(s)$ is Bohr almost periodic and bounded on any vertical strip whose closure lies inside the half plane of uniform convergence $\sigma > \sigma_u(F)$.

We recall that a general Dirichlet series (D-series for short) is of the form

$$F(s) = \sum_{n=1}^{\infty} a(n)e^{-\lambda_n s} \tag{2}$$

with coefficients $a(n) \in \mathbb{C}$ and a strictly increasing sequence of real exponents $\Lambda = (\lambda_n)$ satisfying $\lambda_n \to \infty$. The case $\lambda_n = \log n$ recover the ordinary Dirichlet series. A basis for a D-series is a sequence of real numbers $B = (\beta_l)$ that satisfies the following three conditions:
-the elements of B are $\mathbb{Q}$-linearly independent;
-every λ_n is a $\mathbb{Q}$-linear combination of elements of B;
- every β_l is a $\mathbb{Q}$-linear combination of elements of Λ.
This can be expressed in matrix notation by considering Λ, B as column vectors, and writing the last two conditions as $B = T\Lambda, \Lambda = RB$, where R, T are some Bohr matrices, whose row entries are rational numbers and almost always 0; R is uniquely determined by Λ and B. We say that two D-series $F(s) = \sum_{n\geq 1} a(n)e^{-\lambda_n s}, G(s) = \sum_{n\geq 1} b(n)e^{-\lambda_n s}$, with same exponents Λ, are equivalent if there exist a basis B of Λ and a real column vector $Y = (y_l)$ such that

$$b(n) = a(n)e^{i(RY)_n}, \tag{3}$$

where R is the Bohr matrix related to Λ and B. We observe that in the case of ordinary Dirichlet series with coefficients $a(n), b(n)$, the equivalence relation reduces to the existence of a completely multiplicative function $\rho(n)$ such that $b(n) = a(n)\rho(n)$ for all $n \geq 1$ and such that $|\rho(p)| = 1$ if $p|n$ and $a(n) \neq 0$.
We say that a D-series $F(s)$ or a sequence of exponents Λ has an integral basis if there exists a basis B of Λ such that the associated Bohr matrix R has integer entries. Such basis B is called an integral basis of $F(s)$ or of Λ. Note that an ordinary Dirichlet series ($\Lambda = (\log n)$) has an integral basis ($B = (\log p)$).
We extend the notion of equivalence to vectors in the following way: let $N \geq 1$ and for $j = 1, \ldots, N$ let $F_j(s), G_j(s)$ be two D-series with coefficients $a_j(n), b_j(n)$ respectively and the same exponents Λ. We say

that the vectors $(F_1(s), ..., F_N(s))$ and $(G_1(s), ..., G_N(s))$ are equivalent if exist a basis B of Λ and a real vector $Y = (y_l)$ such that

$$b_j(n) = a_j(n)e^{i(RY)_n}, \forall j = 1, ..., N \tag{4}$$

where R is the Bohr matrix related to Λ and B.
Before state the main result we recall a fundamental result of Bohr theory; see Bohr [1].

Theorem 1 (Bohr's equivalence theorem) *Let $F(s), G(s)$ be equivalent D-series with abscissa of absolute convergence σ_a. Then in any open half plane $\sigma > \sigma_1 > \sigma_a$ the functions $F(s), G(s)$ take the same set of values.*

Now we state the main result; see the paper of Perelli-Righetti [4].

Theorem 2 (Perelli-Righetti) *Let $N \geq 1$ and, for $j = 1, ..., N$, let $F_j(s)$ be general D-series with coefficients $a_j(n)$ and the same exponents Λ, with an integral basis and with finite abscissa of uniform convergence $\sigma_u(F_j)$. Further, let K_j be compact sets inside the half planes $\sigma > \sigma_u(F_j)$ containing at least one accumulation point and let $f_j(s)$ be holomorphic on K_j. Then the following assertions are equivalent:*
i) For every $\varepsilon > 0$ there exists $\tau \in \mathbb{R}$ such that

$$\max_{j=1,...,N} \max_{s \in K_j} |F_j(s + i\tau) - f_j(s)| < \varepsilon; \tag{5}$$

ii) $f_1(s), ..., f_N(s)$ are D-series with exponents Λ, and $(f_1(s), ..., f_N(s))$ is vector equivalent to $(F_1(s), ..., F_N(s))$;
iii) for every $\varepsilon > 0$ we have

$$\liminf_{T\to\infty} \frac{1}{2T} |\{\tau \in [-T, T] : \max_{j=1,...,N} \max_{s \in K_j} |F_j(s + i\tau) - f_j(s)| < \varepsilon\}| > 0; \tag{6}$$

iv) $f_j(s)$ has analytic continuation to $\sigma > \sigma_u(F_j)$ and there exists a sequence τ_k such that $F_j(s + i\tau_k)$ converges uniformly to $f_j(s)$ on every closed vertical strip in $\sigma > \sigma_u(F_j)$, $j = 1, ..., N$.

Note that Theorem 2 holds for ordinary Dirichlet series. Moreover, note that it represents the counterpart of the universality theorems of L-functions in the critical strip. Indeed, Theorem 2 gives a complete characterization of the analytic functions $f_j(s)$ approximable by such translates as in i) and, by Theorem 1 and its converse for D-series with an integral basis (see Righetti [5]), we see that such functions $f_j(s)$ are those assuming the same set of values of the $F_j(s)$'s on any vertical strip inside the domain of absolute convergence. Finally, thanks to iv), such $f_j(s)$'s have analytic continuation to $\sigma > \sigma_u(F_j)$.
We conclude with some remarks about the relevance of integral bases in Theorem 2. Arguing in a similar way as in the proof of Theorem 1 and Theorem 2 one can prove the following

Theorem 3 *Under the assumption of Theorem 2, with Λ not necessarily having an integral basis, suppose that i) holds. Then the $f_j(s)$'s are D-series with coefficients $b_j(n)$ and the same exponents Λ satisfying the following properties: for $j = 1, ..., N$*

$$|b_j(n)| = |a_j(n)|, \sigma_u(f_j) = \sigma_u(F_j) \tag{7}$$

and the set of values of f_j and of F_j on any open vertical strip inside $\sigma > \sigma_u(F_j)$ coincide. Moreover, i) holds for the $f_j(s)$'s described in ii) of Theorem 2.

Similar remarks and variants, namely without assuming the existence of an integral basis, apply also to the equivalence of i) with iii) and iv) in Theorem 2. However, $f_j(s)$ may not be equivalent to $F_j(s)$, as shown by the following example by Bohr [2, pp.151-153]. Let

$$\lambda_n = 2n - 1 + \frac{1}{2(2n-1)}, F(s) = \sum_{n=1}^{\infty} e^{-\lambda_n s}, f(s) = -F(s). \tag{8}$$

In this case, since every λ_n is rational, all bases B of Λ consist of a single rational number, and since the least common multiple of the denominators of the λ_n is ∞, no one is an integral basis. Moreover, the Bohr matrix R, relative to Λ and B reduces to an infinite column vector, hence the vectors Y reduce to a single real number; thus the set of D-series equivalent to $F(s)$ consists of its vertical shifts. Further, as shown by Bohr, $f(s)$ is not equivalent to $F(s)$. On the other hand, $f(s)$ satisfies i) in Theorem 2.

References

[1] H.Bohr *Zur Theorie der allgemeinen Dirichletschen Reihen*, Math. Ann. **79** (1918), 136-156.

[2] A.A.Karatsuba, S.M.Voronin *The Riemann Zeta-Function*, de Gruyter 1992.

[3] K.Matsumoto *A survey on the theory of universality for zeta and L-functions*, In Number Theory: Plowing and Starring Through High Wave Forms, ed. by M.Kaneko *et al.*, p.95-144, World Scientific 2015.

[4] A.Perelli, M.Righetti *A rigidity theorem for translates of uniformly convergent Dirichlet series*, preprint arXiv: 1702.01683.

[5] M.Righetti *On Bohr's equivalence theorem*, J.Math. An. Appl. **445** (2017), 650-654; corrigendum ibid **449** (2017), 939-940.

[6] S.M.Voronin *A theorem on the "universality" of the Riemann zeta-function*, (Russian) Izv. Akad. Nauk SSSR Ser. Math. **39** (1975), 475-486. English transl. Math. USSR-Izv. **9** (1975), 443-453.

Daniele Mastrostefano
Dipartimento di Matematica
Università di Padova
Via Trieste, 63
35131, Padova, Italy.
email: danymastro93@hotmail.it

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 3, *Number* 1, *March* 2018, *pages* 31-36

Christian Maire

Analytic Lie extensions of number fields with cyclic fixed points and tame ramification

(Joint work with Farshid Hajir)

Written by Frances Odumodu

1 Introduction

The conjecture of Fontaine and Mazur characterises all Galois representations which "come from algebraic geometry", that is, representations which arise as Tate twists of the action of G_K on subquotients of étale cohomology of some smooth projective varieties defined over K. The conjecture states that these representations are precisely the *geometric* representations, that is, representations which are unramified outside a finite set S of places v of K and which are *potentially semistable* at all places in S, that is, the restriction of ρ to the decomposition group at each place of K of residual characteristic p becomes semistable (in the sense of Fontaine). The *tame conjecture* of Fontaine and Mazur of ([3], conj 5a) considers only finitely and tamely ramified p-adic representations. Now, fix a prime $p > 3$. The conjecture is as follows

Conjecture 1.1 (Fontaine-Mazur) *Let K be a number field with absolute Galois group $G_K = Gal(\bar{K}/K)$. Let $\rho : G_K \longrightarrow GL_n(\mathbb{Q}_p)$ be a continuous Galois representation such that*

1. *the representation is finitely ramified (that is, the set of ramified primes of ρ is finite).*
2. *ρ is unramified at p*

Then, the image of ρ is finite.

The philosophy of the conjecture: with the hypothesis of the nonramification at p, the eigenvalues of the Frobenius should be roots of unity. In this case, the image of ρ is solvable and by class field theory, the image is finite.

Definition 1.1 *A group Γ is uniform if and only if the following conditions are satisfied*

1. *Γ is a pro-p-group, that is, a projective limit of a finite p-group.*
2. *The commutator $[\Gamma, \Gamma] \subseteq \Gamma^p$; where Γ^p is the subgroup generated by the p-power of elements of Γ.*
3. *Γ is torsion-free.*

The first result in the direction of the conjecture is the following due to Boston [2]:

Theorem 1.1 (Boston) *Let K be a quadratic extension of k with Galois group $\langle\sigma\rangle$. Suppose that there is a uniform Galois extension L of K with Galois group Γ such that L/K is unramified and L/k is Galois. Suppose that the p-part of the classgroup of k is trivial, that is that p is relatively prime to the class number of k, then Γ is trivial.*

Thus, there is no arithmetic in such situation. Note that a uniform group is a special case of an analytic group. A p-adic analytic group is a closed subgroup of $GL_m(\mathbb{Z}_p)$ for some integer m. Lazard relates uniform groups and p-adic analytic groups in [1]:

Theorem 1.2 (Lazard) *Let G be a p-adic analytic pro-p group. Then G contains an open uniform subgroup.*

As G is compact, "open" means "of finite index". For the conjecture of Fontaine-Mazur, one has to prove that something is finite, thus we can reduce to the case where the image of ρ is uniform.

The main ingredients of the proof of Boston. The element σ acts on Γ and since p is coprime to the class number of K, we have that σ does not act trivially on the abelianization $\Gamma^{ab} = \Gamma/[\Gamma, \Gamma]$. That is the action of σ on Γ^{ab} is fixed point free. As Γ is uniform, σ does not act trivially on Γ. Since σ has order 2 which is coprime to p and Γ is a pro-p group, we have that Γ is solvable and by class field theory, Γ is necessarily finite. By the definition of uniformity, Γ is torsion free. Hence, Γ is trivial.

This is not always the case: For example, consider the same situation. We know how to construct some extension where the Hilbert classfield tower is infinite. Here K_∞ is the p-Hilbert class field tower of K. Recall that the class group of $\mathbb{Q}$ is trivial. Now, σ does not act trivially on G^{ab} but the action of σ on G has some fixed points, that is, points $g \in G$ such that $\sigma(g) = g$ with $g \neq 1$. If there were no fixed points under the action of σ on G, the conclusion would be the same. That is, G should be solvable and then finite. But this is not the case. This is very particular to the uniform situation.

$$\begin{tikzcd}
K_\infty \arrow[d, dash, "G"] \\
\mathbb{Q}(\sqrt{\pm d}) \arrow[d, dash, "\langle\sigma\rangle"] \\
\mathbb{Q}
\end{tikzcd}$$

2 Uniform situation

What happens if we add some fixed points following the action of σ on Γ with Γ uniform. The context of Boston is "no fixed points". So here we add some fixed points.

Examples of uniform groups The first uniform group that is nontrivial for the Fontaine-Mazur conjecture is

$$SL_2^1(\mathbb{Z}_p) = ker(SL_2(\mathbb{Z}_p) \to SL_2(\mathbb{F}_p)).$$

This group is uniform of dimension 3. More generally, the group $SL_n^1(\mathbb{Z}_p) = ker(SL_n(\mathbb{Z}_p) \to SL_n(\mathbb{F}_p))$ is uniform of dimension $n^2 - 1$. We would like to obtain new uniform groups in the direction of the Fontaine-Mazur conjecture.

Class field towers. Let K be a number field and S a finite set of places of K. Let K_S be the maximal pro-p-extension of K unramified outside S, and $G_S = G_S(K) = Gal(K_S/K)$ be its Galois group. This extension is too big so we cut it. Let T be a finite set of places of K disjoint with S. Let K_S^T be the maximal extension of K such that there is no ramification outside S and every place in T splits totally. Put $G_S^T = Gal(K_S^T/K)$ be its Galois group.

We generalise the context of Boston, that is, look at the action of an element σ of order ℓ coprime to p. To simplify the exposition, take $\ell = 2$. We first define the concept of a σ-uniform image.

Definition 2.1 *Consider a continuous Galois representation*

$$\rho : G_S^T \to GL_n(\mathbb{Z}_p).$$

Let L be the subfield of K_S^T fixed by $\ker(\rho)$ *such that $\Gamma = im(\rho)$ is naturally identified with $Gal(L/K)$. Then, Γ is said to be σ-*uniform *if $\Gamma = Gal(L/K)$ is uniform and the extension L/k is Galois.*

Theorem 2.1 (Hajir-Maire) *Let K be a quadratic extension of k. Suppose that s is a positive integer and that p does not divide the order of Cl_K. Let T be a set of primes of K sufficiently large, that is, the order of T satisfies $|T| \geq \alpha s + \beta$ with α, β constants depending on K. Then there exist s sets $S_1, \ldots, S_s$ of places of K, of positive (Chebotarev) density such that for every finite set $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$ of places of K with $\mathfrak{p}_i \in S_i$, we have the following*

1. *The arithmetic is nontrivial. That is, $G_S^T(K)$ is infinite.*

2. *Under the action of σ on $(G_S^T)^{ab}$, there are s independent fixed points.*

3. *There is no continuous Galois representation $\rho : G_S^T \to GL_n(\mathbb{Z}_p)$ with σ-uniform image $SL_2^1(\mathbb{Z}_p)$ if:*

   a) Fontaine-Mazur conjecture holds for the base field k.
   or

   b) $s \leq 2$ ("small").

If we replace $SL_2^1(\mathbb{Z}_p)$ with $SL_n^1(\mathbb{Z}_p)$, the result still holds and we have $s \leq n^2 - 1$, if the action of σ on the group Γ corresponds to σ_A, conjugation by a matrix $A \in GL_n(\mathbb{Z}_p)$.

Sketch of proof. The first statement is a consequence of Golod-Shafarevich since $|T|$ grows linearly with s.

For the second statement, we need the following. Let K^H be the p-Hilbert class field of K, that is, the maximal abelian unramified p-extension of K. Let $Cl_K(p)$ be the p-sylow classgroup of K and $N = Gal(K^H/K)$. Then, Artin map gives the canonical isomorphism $Cl_K(p) \cong N$. The prime p divides the order of N, so we are not in the semisimple case.

$$\begin{tikzcd}
K^H \arrow[d, dash, "\cong Cl_K(p)"] \\
K \arrow[d, dash, "\langle\sigma\rangle"] \\
k
\end{tikzcd}$$

We want to choose S in order to create enough fixed points for the action of σ. To find S we use Kummer theory and Chebotarev density theorem. To do this, we need to know more about the units $\mathcal{O}$ of K^H. The arithmetic question is to find a Minkowski unit from the extension K^H/K. Now, K^H has a Minkowski unit if $\mathcal{O}/(\mathcal{O})^p$ contains a nontrivial $\mathbb{F}_p[N]$-free module. We look at the structure of the units of K^H modulo p as an $\mathbb{F}_p[N]$-module. We introduce the set T and consider the T-units $\mathcal{O}^T$. We prove that when T is large, the T-units admit a large $\mathbb{F}_p[N]$-module.

Thus, we compare the Galois module structure coming from group theory by the action of σ on some subgroup of the analytic group, with the structure coming from arithmetic structure and by the choice of S, there is an incompatibility.

References

[1] Michel Lazard. *Groupes analytiques p-adiques*. Publications mathématiques de l'I.H.É.S., tome 26 (1965), p.5-219.

[2] Nigel Boston. *Some cases of the Fontaine-Mazur conjecture*. Journal of Number Theory 42 (1992), p. 285-291.

[3] Jean-Marc Fontaine and Barry Mazur. *Geometric Galois representations* in *Elliptic curves, modular forms and Fermat's last theorem*. Proceedings of a conference at the institute of mathematics of the chinese university of Hongkong. Ed, J. Coates and S.T. Yau. International press, (1997), p. 190-227.

[4] Farshid Hajir and Christian Maire. *Analytic Lie extensions of number fields with cyclic fixed points and tame ramification*. Preprint. 2017

Frances Odumodu
Institut de Mathematiques de Bordeaux
Universite de Bordeaux
351 cours de la liberation
33400 Talence, France.
email: `francesodumodu@gmail.com`

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 3, *Number* 1, *March* 2018, *pages* 37-44

Pieter Moree

Counting constrained almost primes

written by Carlo Pagano

1 General problem and main results

As the title suggests, this talk was concerned with asymptotic problems on *constrained k-almost primes*, where k is a fixed positive integer.

A positive integer n is said to be k-almost prime if $\Omega(n) = k$, i.e. if n has precisely k prime factors counted with multiplicities (for example 6 and 9 are both 2-almost prime). The *constrained* refers to the fact that additional constraints will be considered on the prime factors constituting the number n. As we shall see in the next section, the motivation of constraining the prime factors of n comes from the two main applications of this subject, namely cryptography and a problem about the size of the coefficients of the cyclotomic polynomials.

For a positive real number x, define

$$\pi(x, k) := \#\{n \leqslant x : \omega(n) = k\},\ N(x, k) := \#\{n \leqslant x : \Omega(n) = k\},$$

where $\omega(n)$ denotes the number of prime factors of n without multiplicity. By definition $N(x, k)$ is precisely the number of k-almost prime integers up to x. The two functions have the same order of magnitude, which is established in a classical theorem of Landau [6].

Theorem 1 (Landau, 1909)**.** *Let k be a fixed positive integer. Then, asymptotically in x,*

$$\pi(x,k) \sim N(x,k) \sim \frac{x}{\log(x)} \frac{(\log\log(x))^{k-1}}{(k-1)!}.$$

We recall that given two functions $A_1(x)$ and $A_2(x)$ the notation $A_1(x) \sim A_2(x)$ is a shorthand for

$$\lim_{x\to\infty} \frac{A_1(x)}{A_2(x)} = 1.$$

The speaker stressed that this is only the easiest version of a broad spectrum of results of Erdős, Sathe, Selberg, Hensley and Hildebrand-Tenenbaum, valid on larger regions of the plane (x,k).

Clearly for $k = 1$ one recovers (a simple version of) the prime number theorem, which in its cruder form states that the counting of the number of primes up to x, i.e. $\pi(x,1)$, satisfies

$$\pi(x,1) \sim \frac{x}{\log(x)}.$$

With an eye towards applications, the rest of the talk has been focused on the cases $k = 2$ and $k = 3$ with the constraints that we next explain.

1.1 Binary integer with prime factors within a given factor

Fix $r > 1$ a real number. Denote by

$$C_r(x) := \#\{pq \leqslant x : p < q < rp\}.$$

In words, this is the set of square-free 2-almost prime numbers, whose 2 distinct prime factor are within each other of a multiplicative factor at most r. Decker and the author [1] dubbed these integers `RSA-integers`, as integers with two prime factors of roughly the same size play an important role in the RSA cryptosystem. One of the two goals of the talk was to show recent results that the author obtained regarding the asymptotic evaluation of $C_r(x)$. In increasing precision of the asymptotic formula, one has:

Theorem 2 (Decker and Moree, [1]). *As x tends to infinity we have*

$$C_r(x) = \frac{2x \log\log(r)}{(\log(x))^2} + O\Big(\frac{rx\log(er)}{(\log(x))^3}\Big).$$

Theorem 3 (Moree and Saad Eddin, [5]). *For $x \geqslant 2r$ and x tending to infinity we have*

$$C_r(x) = \int_{2r}^{x} \frac{\log\log(\sqrt{rt}) - \log\log(\sqrt{\frac{t}{r}})}{\log(t)} + O(rxe^{-c_1\sqrt{\log(x)}})$$

for some constant $c_1 > 0$.

By partial integration one obtains from the latter result:

Theorem 4 (Moree and Saad Eddin [5]). *Let $r > 1$ be an arbitrary fixed real number and $n \geqslant 2$ be an arbitrary integer. As x tends to infinity, we have*

$$C_r(x) = \sum_{j=1}^{n-1} a_j(r)\frac{x}{(\log(x))^{k+1}} + O_n\Big(\frac{x\log(2r)^{2\lfloor n/2\rfloor+1}\log(r)}{(\log(x))^{n+1}}\Big) + O(rxe^{-c(\varepsilon)\sqrt{\log(x)}}).$$

Where $c(\varepsilon) = (1-\varepsilon)c/\sqrt{2}$, for a constant $c > 0$ and $0 < \varepsilon < 1$ is arbitrary, and where

$$a_k(r) := \sum_{j=1}^{[\frac{k+1}{2}]} \frac{k!}{(2j-1)!}\frac{2\log(r)^{2j-1}}{2j-1}.$$

Here $[x]$ denotes the integral part of x and $\lfloor x \rfloor$ its floor.

1.2 Binary integers within a given factor and in a given congruence

The results of this section are motivated by a recently observed *bias* in the congruence of the two factors of a binary integer modulo 4. Namely consider the counting function

$$s(x) := \frac{\#\{pq \leqslant x : p \equiv q \equiv 3 \bmod 4\}}{\frac{1}{4}\#\{pq \leqslant x\}}.$$

One would obviously expect that numerical simulation should show rather rapidly that $s(x)$ approaches to 1. So it might be quite surprising that one finds numerically that $s(10^6)$ is roughly 1.183 and $s(10^7)$ is roughly 1.162. This suggested the presence of a large *secondary term*, as indeed can be proved:

Theorem 5 (Dummit, Granville and Kisilevsky [2])**.**

$$s(x) = 1 + \frac{\beta + o(1)}{\log\log(x)},$$

with β of order 0.334 *up to the third decimal digit.*

Clearly the theorem explains the above empirical bias, as $\beta/\log\log(x)$ decreases immensely slowly to zero!

Given the cryptography-application of binary integers of the restricted form discussed in the previous subsection called RSA-integers, it is interesting to see if they display a similar bias. If so one might perhaps be able to speed up cracking the RSA-system by assuming that both prime factors are congruent to 3 modulo 4 first.

The result obtained is as follows:

Theorem 6 (Moree and Saad Eddin [5])**.** *Let a_1, d_1, a_2, d_2 be natural numbers with $(a_1, d_1) = (a_2, d_2) = 1$. Set*

$$\mathcal{S}(x) = \{pq \leqslant x : p \equiv a_1 \bmod d_1, q \equiv a_2 \bmod d_2\}.$$

We then have:

$$\frac{\#\mathcal{S}(x)}{\frac{1}{\phi(d_1)\phi(d_2)}\#\{pq \leqslant x\}} = 1 + O_r\big((\log(x))^2 e^{-c(\varepsilon)\sqrt{\log(x)}}\big).$$

Note that the error decreases very quickly to zero and thus there is at most a very weak bias. In particular, there is no usable bias in the RSA-integer case (with $d_1 = d_2 = 4$).

1.3 Ternary integers

Consider the constrained ternary problem of asymptotically estimating the cardinality of

$$\mathcal{T}(x)=\{pqr \leqslant x : 3 \leqslant p < q < r < \frac{p-1}{p-2}(q-1), r \equiv q \equiv \pm 1 \bmod p\}.$$

The speaker, together with a number of coauthors, obtained the following result [4]:

Theorem 7 (Luca, Moree, Osburn, Saad Eddin and Sedunova, 2017)**.** *We have that*

$$\#\mathcal{T}(x) = C_1 \frac{x}{(\log(x))^2} + O\Big(\frac{x \log\log(x)}{(\log(x))^3}\Big),$$

where

$$C_1 = \frac{1}{4}\sum_{l \geqslant 3} \frac{1}{l(l-1)^2} \log\Big(\frac{l-1}{l-2}\Big),$$

with l running over all odd prime numbers.

2 Motivation and applications

2.1 Motivation

The security of the RSA system is based on the fact that (with classical computers) it is considered difficult to factor RSA-integers in reasonable time. This motivated the speaker to estimate the number of such integers up to x and to see how much of a bias there is when congruence conditions are specified for the two prime factors.

2.2 Applications

Let n be a positive integer. Let $\zeta_n := e^{\frac{2\pi i}{n}}$. Recall that the n-th cyclotomic polynomial is defined as

$$\Phi_n(T) = \prod_{1 \leqslant j \leqslant n, (j,n)=1} (x - \zeta_n^j).$$

We will look at its coefficients:

$$\Phi_n(T) := \sum_{i=0}^{\phi(n)} a_n(i) T^i,$$

where $\phi(n)$ denotes Euler's totient function. One defines the height of $\Phi_n(T)$ to be the largest value of $|a_n(i)|$ as i ranges through $\{0, \ldots, \phi(n)\}$.

It is a known fact that $A(n) = 1$ whenever n is at most binary. Then one has to look at at least ternary integers to see some non-trivial behaviour.

It was proven by Bang, in 1895, that $A(pqr) \leqslant p-1$, for $p < q < r$. Therefore one has that $\max_{q,r}\{A(pqr : p < q < r\}$ exists; denote it by $M(p)$. It is the main open problem in the subject, to determine a formula or an efficient algorithm to compute $M(p)$. It has been conjectured by a Sister, named Sister Beiter, that $M(p) \leqslant \frac{p+1}{2}$. This conjecture has been disproved by the speaker and Gallot in 2008 [3] for all primes p. They proposed a corrected version of this conjecture, by conjecturing that $M(p) \leqslant \frac{2}{3}p$. They called this the *corrected Beiter conjecture*. They were able to show that, given an $\varepsilon > 0$, the inequality $M(p) > (2/3 - \varepsilon)p$ holds for all large enough p.

Using Theorem 7, the authors of [4] established the following result.

Theorem 8 (Luca, Moree, Osburn, Saad Eddin and Sedunova (2017))**.** *The number $T(x)$ of ternary $n = pqr \leqslant x$ such that $A(pqr) \leqslant \frac{2p}{3}$ satisfies*

$$T(x) \geqslant \Big(\frac{25}{27} + o(1)\Big)\pi(x,3) \geqslant \Big(\frac{25}{27} + o(1)\Big)\frac{x(\log\log(x))^2}{2\log(x)}.$$

This implies that a very big proportion of the ternary integers $\leq x$, namely at least 0.925 for all x large enough, respects the corrected Beiter conjecture, that is

$$|a_{pqr}(i)| \leqslant \frac{2}{3}p \text{ for each } i \in \{0, \dots, \phi(pqr)\}.$$

References

[1] A. Decker and P. Moree, *C*ounting RSA-integers, Result. Math. **5**2 (2008), 35–39.

[2] D. Dummit, A. Granville, and H. Kisilevsky, Big biases amongst product of two primes, *M*athematika **6**2, (2016), 502–507.

[3] Y. Gallot and P. Moree, Ternary cyclotomic polynomials having a large coefficient, *J*. Reine Angew. Math. **6**32 (2009), 105–125.

[4] F. Luca, P. Moree, R. Osburn, S. Saad Eddin, and A. Sedunova, Constrained ternary integers, `arXiv:1710.08403`, (2017).

[5] P. Moree and S. Saad Eddin, Products of two proportional primes, *I*nt. J. Number Theory **1**3 (2017), 2583–2596.

[6] G. Tenenbaum, Introduction to analytic and probabilistic number theory, *C*ambridge University Press, (1995).

Carlo Pagano
Mathematisch Instituut
Universiteit Leiden
Niels Bohrweg 1
2333 CA Leiden, The Netherlands.
email: c.pagano@math.leidenuniv.nl

For $n \geqslant 2$, let K_n be the Hilbert of K_{n-1}: $K_n = (K_{n-1})_1$. The tower $K \subset K_1 \subset K_2 \subset \dots$ is called Hilbert tower of K.

$$\begin{tikzcd}
K_\emptyset \arrow[d, dotted, no head] \arrow[ddd, bend right=40, no head, "G_\emptyset"'] \\
K_2 = (K_1)_1 \arrow[d, no head] \\
K_1 \arrow[d, no head] \arrow[d, bend left=40, no head, "A(K)"] \\
K
\end{tikzcd}$$

Remark. The question of the finiteness of Hilbert class field towers had been discussed by Artin and Hasse in their correspondence. It appears that Artin doubted the existence of an infinite Hilbert tower.

By construction, for every index $n \geqslant 2$, the intermediate Galois group $\mathrm{Gal}(K_n|K_{n-1})$ is isomorphic to the p-class group $A(K_{n-1})$ of the field K_{n-1}. The Fontaine Mazur conjecture predicts that the p-rank of $A(K_n)$ goes to infinity. Is its growth due to the growths of both $|A(K_n)|$ and $\mathfrak{m}_{A(K_n)}$, or can we find some situations where the average exponent is bounded?

The aim of this last part is to construct an example of an infinite tower of unramified Galois extensions $K \subset K_1 \subset \dots$ such that $\mathfrak{m}_{A(K_n)}$ remains bounded above. Recall that the average exponent $\mathfrak{m}_{A(K_n)}$ is defined as the quotient $\log_p(|A(K_n)|)/d(A(K_n))$. This idea is then simple: the first step is to make $d(A(K_n))$ grow as fast as possible, and the second step is to find an upper bound for the numerator.

$$\begin{tikzcd}
& & & & k_{\emptyset} \\
& K_n \arrow[dl, dash] \arrow[dr, dash] & & k_{\emptyset}^{T} \arrow[ur, dash] & \\
K \arrow[dr, dash] & & k_n \arrow[dl, dash] \arrow[ur, dash] & & \\
& k \arrow[d, dash] & & & \\
& \mathbb{Q} & & &
\end{tikzcd}$$

Under these hypothesis, for all $n \geqslant 1$, $d(A(K_n))$ is bounded from below by $t[k_n : k] - 1$. By section 3.2.1, we then know that $d(A(K_n))$ grows linearly with the degree of the extension $K_n|K$. Using what has been done before, we obtain for the numerator the following:

$$\begin{aligned}
\log_p(|A(K_n)|) &\leqslant \log_p(h_{K_n} R_{K_n}) - \log_p R_{K_n} \\
&\leqslant 1.0765 \log_p(\sqrt{|d_{K_n}|}) \\
&\leqslant 1.0765 \log_p(\sqrt{|d_K|})[K_n : K] \\
&\leqslant 1.0765 \log_p(\sqrt{|d_K|})[k_n : k] \\
&\leqslant 1.0765 \log_p(\sqrt{|d_K|}) \frac{d(A_{K_n})}{t}.
\end{aligned}$$

Finally :

$$\begin{aligned}
\mathfrak{m}_{A(K_n)} = \frac{\log_p(|A(K_n)|)}{d(A(K_n))} &\leqslant \frac{1.0765 \log_p(\sqrt{|d_K|}) \frac{d(A_{K_n})}{t}}{d(A(K_n))} \\
&\leqslant \frac{1.0765 \log_p(\sqrt{|d_K|})}{t}.
\end{aligned}$$

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 3, *Number* 1, *March* 2018, *pages* 45-53

Farshid Hajir

On exponents of class groups in towers of number fields

Written by Marine Rougnant

The Talk is based on a joint work with Christian Maire.

1 Ideal class groups

The ideal class group of a number field K, denoted Cl_K, is the quotient of the fractional ideals of the integer ring $\mathcal{O}_K$ by the the subgroup of principal ideals. Its cardinality h_K, called the class number of K, measures how far $\mathcal{O}_K$ is from a principal ring, and is also a measure of the obstruction to the uniqueness of a decomposition of an ideal into a product of prime ideals.

The ideal class groups are quite simple to define but they are still very mysterious. It is known that the class number of a number field K is always finite and Minkowski's bound permits to compute the class group of a given field K. Despite this, most of the questions on infinite families of fields are still open. For example, are there infinitely many number fields K (up to isomorphism) with principal integer ring or, at least, with h_K bounded by a given number? Or can we show that there are infinitely many number fields with cyclic class group, or even with class group generated by, say, 2017 elements?

Even if we are no able yet to give an answer to any of these questions, we can point to some great advances in understanding variation of class groups in towers. We must first quote Iwasawa's formula, which gives asymptotically the growth of the p-part of ideal class groups in a $\mathbb{Z}_p$-extension. On the other hand, Cohen-Lenstra heuristics give an overall approach to predicting the distributions of class groups in certain situations; recent advances by Bhargava and his collaborators have verified a growing body of Cohen-Lenstra type predictions.

One is quickly led to study ideal class groups one p-part at a time. Let us fix notations for the rest of the paper. Let $p > 2$ be an odd prime number; let K be a number field. We will denote by Cl_K the ideal class group of K and by $A(K)$ the p-Sylow subgroup of Cl_K, that we call p-class group of K.

2 Average exponent

Throughout, we take $p > 2$ to be an odd prime. The structure theorem of finite abelian groups says that every finite abelian p-group A can be written as a product of cyclic p-groups: letting $d = d(A)$ be the dimension of the $\mathbb{F}_p$-vector space A/pA, there exist d positive integers $a_1 \geqslant \ldots \geqslant a_d$ such that

$$A \simeq \mathbb{Z}/p^{a_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p^{a_{d(A)}}\mathbb{Z}.$$

We recall that the exponent of A is defined as the maximal order p^{a_1} of its elements.

We then have:

$$|A| = \prod_{i=1}^{d(A)} p^{a_i}.$$

Definition. The logarithmic average exponent of a finite p-group A is given by

$$\mathfrak{m}_A = \log_p(|A|^{1/d(A)}).$$

In particular, it follows from this definition that $\log_p |A| = \mathfrak{m}_A d(A)$.

3 Towers of number fields

3.1 Abelian p-adic analytic extensions : Iwasawa's formulas

$$\begin{tikzcd}
L \arrow[d, dotted, no head] \arrow[ddd, bend right, no head, "\mathbb{Z}_p"'] \\
K_{n+1} \arrow[d, no head] \\
K_n \arrow[d, dotted, no head, "p^n"] \\
K
\end{tikzcd}$$

Let K be a number field and $L|K$ a $\mathbb{Z}_p$-extension of K, i.e. a Galois extension of K whose Galois group is isomorphic to $\mathbb{Z}_p$. The closed subgroups of $\mathbb{Z}_p$ are exactly the groups $p^n\mathbb{Z}_p$ for $n \geqslant 0$; hence for each such n, there exists a unique subextension $K_n|K$ of $L|K$ of degree p^n.

Iwasawa's formulas give the asymptotic behavior of the p-rank and of the cardinality of the groups $A(K_n)$:

Theorem. *There exist $\mu, s_\mu, \lambda \geqslant 0$ (depending on L) and $\nu \in \mathbb{Z}$ such that for all large enough n,*

1. $\log_p |A(K_n)| = \mu p^n + \lambda n + \nu$,
2. $d(A(K_n)) = s_\mu p^n + O(1)$.

We can deduce from the second point that if μ is 0, then the p-rank is bounded. It follows that $\mathfrak{m}_{A_n}$ goes to infinity if $\mu = 0$ and $\lambda \neq 0$. This observation leads us to consider a particular $\mathbb{Z}_p$-extension.

Adjoining to the field K all the roots of unity with order a power of p, we define a Galois extension $K(\mu_{p^\infty})|K$. We call cyclotomic $\mathbb{Z}_p$-extension of K the unique subfield $K_\infty|K$ corresponding to the maximal pro-p quotient of $\mathrm{Gal}(K(\mu_{p^\infty})|K))$. This $\mathbb{Z}_p$-extension of K is wildly ramified at least at one prime above p.

$$\begin{tikzcd}
 & K(\zeta_p) \arrow[r, dash] & K(\zeta_{p^2}) \arrow[r, dash] & K(\zeta_{p^3}) \arrow[r, dash, dotted] & {} \\
K \arrow[ur, dash, "\text{degree}|(p-1)"] \arrow[r, dash, "p"] & F_1 \arrow[ur, dash] \arrow[r, dash, "p"] & F_2 \arrow[ur, dash] \arrow[r, dash, dotted] & {}
\end{tikzcd}$$

Iwasawa conjectured that the invariant μ of the cyclotomic $\mathbb{Z}_p$-extension of a number field would be 0 and proved it in the case where K is $\mathbb{Q}$. This theorem was extended by Ferrero and Washington for abelian extensions of $\mathbb{Q}$. The last conjecture we have to mention about cyclotomic $\mathbb{Z}_p$-extensions is the following, due to Ralph Greenberg:

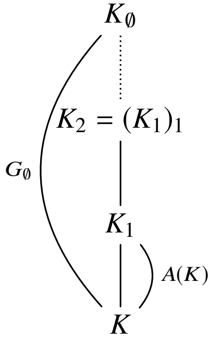
Conjecture. *If K is totally real and if K_∞ is the $\mathbb{Z}_p$-cyclotomic extension of K, then $\lambda = \mu = 0$. In particular $|A(K_\infty)|$, $d(A(K_\infty))$ and $\mathfrak{m}_{K_\infty}$ are bounded.*

3.2 Class field towers : the unramified case

Let K be a number field and let S, T be two finite disjoint sets of places of K. The compositum of all finite p-extensions of K unramified outside S and totally split at the primes of T is still unramified outside S and T-split: this is the maximal pro-p extension of K unramified outside S and T-split. This extension that we denote by K_S^T is Galois (by maximality). Denote by G_S^T (or $G_S^T(K)$) its Galois group. Recall that if $S' \subset S$ and $T \subset T'$, we have $K_{S'}^{T'} \subset K_S^T$.

The study of the unramified case, where S and T are the empty set, was first motivated by geometry: indeed $G_\emptyset$” = ”$\pi_1(SpecO_K)$. Moreover, the pro-p group $G_\emptyset$ is linked to the class group of K by class field theory: Artin's symbole gives and isomorphism between its abelianized $G_\emptyset^{ab}$ and $A(K)$ (we can see $G_\emptyset$ as a non-abelian generalisation of $A(K)$). We denote by K_1 and we call p-Hilbert of K the subfield of $K_\emptyset$ corresponding to $G_\emptyset^{ab}$.

For $n \geqslant 2$, let K_n be the Hilbert of K_{n-1}: $K_n = (K_{n-1})_1$. The tower $K \subset K_1 \subset K_2 \subset \ldots$ is called Hilbert tower of K.



Remark. The question of the finiteness of Hilbert class field towers had been discussed by Artin and Hasse in their correspondence. It appears that Artin doubted the existence of an infinite Hilbert tower.

By construction, for every index $n \geqslant 2$, the intermediate Galois group $\mathrm{Gal}(K_n|K_{n-1})$ is isomorphic to the p-class group $A(K_{n-1})$ of the field K_{n-1}. The Fontaine Mazur conjecture predicts that the p-rank of $A(K_n)$ goes to infinity. Is its growth due to the growths of both $|A(K_n)|$ and $\mathfrak{m}_{A(K_n)}$, or can we find some situations where the average exponent is bounded?

The aim of this last part is to construct an example of an infinite tower of unramified Galois extensions $K \subset K_1 \subset \ldots$ such that $\mathfrak{m}_{A(K_n)}$ remains bounded above. Recall that the average exponent $\mathfrak{m}_{A(K_n)}$ is defined as the quotient $\log_p(|A(K_n)|)/d(A(K_n))$. This idea is then simple: the first step is to make $d(A(K_n))$ grow as fast as possible, and the second step is to find an upper bound for the numerator.

3.2.1 Growth of the denominator

Let $K \subset K_1 \subset \ldots \subset K_n \subset \ldots \subset K_\emptyset$ be an infinite tower of unramified Galois extensions. For any n, the Galois group H_n of the extension $K_\emptyset | K_n$ is a normal subgroup of $G_\emptyset$. We can first use the following result from group theory to show that its p-rank grows at most linearly with the degree of the extension $K_n|K$:

Proposition.*F*or a pro-p group G and an open subgroup H, $d(H) - 1 \leqslant [G : H](d(G) - 1)$, with equality if G is free.

Furthermore, Burnside's basis theorem gives $d(H_n) = d(H_n^{ab})$ so we have finally the following inequality for every n:

$$d(A(K_n)) - 1 \leqslant [K_n : K](d(G_\emptyset) - 1).$$

The p-rank $d(A(K_n))$ can grow at most linearly with the index of H_n in $G_\emptyset$. We now have to make sure that it will grow as fast as possible. Genus theory (and a trick invented by Iwasawa) permits to find a tower where $d(A(K_n))$ grows linearly in $[K_n : K]$ (cf section 3.3).

3.2.2 A bound for the numerator of $\mathfrak{m}_{A_{K_n}}$

By definition, $|A(K_n)|$ is at most h_{K_n}. The well-known Brauer-Siegel theorem gives an asymptotic relation between it and the discriminant of K_n:

Theorem. *(*Brauer-Siegel) Let k be a field ranging over a sequence $\mathcal{K} = (k_n)$ of Galois extensions of $\mathbb{Q}$ such that the root discriminant $rd_{k_n} = |d_{k_n}|^{1/[k_n:\mathbb{Q}]}$ tends to infinity, where $d_(k_n)$ is the discriminant of the field k_n.

Then $B(\mathcal{K}) = \lim_{n\to+\infty} \dfrac{\log(h_{k_n} R_{k_n})}{\log(\sqrt{|d_{K_n}|})}$ exists and is equal to 1.

Unfortunately, the root discriminant rd_{k_n} is constant in an infinite tower of unramified extensions so Brauer-Siegel's theorem cannot apply in our context. Instead, we will use one of its generalizations, due to Tsfasman-Vladut:

Theorem[3]. *If we do not assume the condition on rd_{k_n}, then $B(\mathcal{K})$ exists and is bounded by $1 + C$, where $C \leqslant 0.1588$. If K is totally complex, we can take $C = 1.0764$.*

By definition of $A(K_n)$, we have :

$$\log_p(|A(K_n)|) \leqslant \log_p h_{K_n} = \log_p(h_{K_n} R_{K_n}) - \log_p(R_{K_n}).$$

Tsfasman-Vladut's theorem gives an asymptotic bound of the first summand. It remains to minimize $\log_p(R_{K_n})$, which we get via a fundamental result of Friedman giving an absolute lower bound for the regulator of all numbers fields.

3.3 Example

Let k be a number field and let $T = \{p_1, \dots, p_t\}$ be a finite set of prime numbers. Let (k_n) be a sequence of unramified extensions in which every element of T splits, i.e. such that $k_n \subset k_\emptyset^T$ for every n. Consider the imaginary quadratic field $K = k(\sqrt{-p_1 \dots p_t})$ and, for every n, denote by K_n the compositum Kk_n. In particular, as the extension $K|k$ is linearly disjoint of any unramified extension of k, the degrees $[K_n : K]$ and $[k_n : k]$ are equal.

$$\begin{tikzcd}
 & & & & k_{\emptyset} \\
 & K_n \arrow[dl, dash] \arrow[dr, dash] & & k_{\emptyset}^{T} \arrow[ur, dash] & \\
K \arrow[dr, dash] & & k_n \arrow[ur, dash] \arrow[dl, dash] & & \\
 & k \arrow[d, dash] & & & \\
 & \mathbb{Q} & & &
\end{tikzcd}$$

Under these hypothesis, for all $n \geqslant 1$, $d(A(K_n))$ is bounded from below by $t[k_n : k] - 1$. By section 3.2.1, we then know that $d(A(K_n))$ grows linearly with the degree of the extension $K_n|K$. Using what has been done before, we obtain for the numerator the following:

$$\begin{aligned}
\log_p(|A(K_n)|) &\leqslant \log_p(h_{K_n} R_{K_n}) - \log_p R_{K_n} \\
&\leqslant 1.0765 \log_p(\sqrt{|d_{K_n}|}) \\
&\leqslant 1.0765 \log_p(\sqrt{|d_K|})[K_n : K] \\
&\leqslant 1.0765 \log_p(\sqrt{|d_K|})[k_n : k] \\
&\leqslant 1.0765 \log_p(\sqrt{|d_K|}) \frac{d(A_{K_n})}{t}.
\end{aligned}$$

Finally :

$$\begin{aligned}
\mathfrak{m}_{A(K_n)} = \frac{\log_p(|A(K_n)|)}{d(A(K_n))} &\leqslant \frac{1.0765 \log_p(\sqrt{|d_K|}) \frac{d(A_{K_n})}{t}}{d(A(K_n))} \\
&\leqslant \frac{1.0765 \log_p(\sqrt{|d_K|})}{t}.
\end{aligned}$$

Remark. By using refined results of Tsfasman and Vladut, we are able to create an example of an infinite unramified tower of p-extensions, with $p = 2$, for which $\mathfrak{m}_{A(K_n)} \leqslant 8,858$; it would be very interesting to see how to refine such constructions further to make $\mathfrak{m}_{A(K_n)}$ as small as possible.

References

[1] G. Gras, Class Field Theory, From Theory to practice, Springer-Verlag, Berlin, 2003.

[2] F. Hajir and C. Maire, *On the invariant factors of class groups in towers of number fields*, preprint.

[3] M. Tsfasman and S. Vladut, *Infinite global fields and the generalized Brauer-Siegel theorem*. Dedicated to Yuri I. Manin on the occasion of his 65th birthday. Mosc. Math. J. **2**(2002), no.2, 329–402.

Marine Rougnant
Laboratoire de Mathématiques de Besançon
Université de Bourgogne Franche-Comté
16 route de Gray
25000 Besançon, France.
email: `marine.rougnant@univ-fcomte.fr`

1. One decomposes $\mathcal{M} \otimes_k \mathcal{M}^*$ using the properties of the eigenring (see [8, Proposition 2.40]). This boils down to finding the rational solutions of a differential system of rank n^4, which increases considerably the complexity of the algorithm. Fortunately, there are some canonical decompositions of $\mathcal{M} \otimes_k \mathcal{M}^*$ that allow, for instance, to consider two differential systems of rank $(n^2-1)n^2/2$ and $(n^2-1)(n^2-2)/2$, rather than of rank n^4. In spite of the appearances, it is quite a gain since for $n = 3$ one has to solve two systems of rank 36 and 28, which is already much faster than solving a system of rank 81.

2. One has to select the pieces of the decomposition of $\mathcal{M} \otimes_k \mathcal{M}^*$ containing $\mathfrak{g}^k$. This is done systematically, testing all the proper submodules of $\mathcal{M} \otimes_k \mathcal{M}^*$. So, the algorithm selects a maximal submodule $\mathfrak{g}^{guess}$ and it goes to the next step to test it.

3. The test consists in trying to find the matrix P. There are two possibilities:

   a) It can find P: it means that $\mathfrak{g}^k \subset \mathfrak{g}^{guess}$. Then it goes back to step 2 and tests of all the proper maximal submodules of $\mathfrak{g}^{guess}$ to see if it has to replace $\mathfrak{g}^{guess}$ by a smaller candidate or if we have found $\mathfrak{g}^k$ and P, and therefore $\mathfrak{g}$.

   b) It cannot find P: it means that $\mathfrak{g}^k \not\subset \mathfrak{g}^{guess}$, so it goes back to step 2 and picks another candidate.

References

[1] A. Aparicio Monforte, E. Compoint, and J.-A. Weil. A characterization of reduced forms of linear differential systems. *Journal of Pure and Applied Algebra*, 217(8):1504–1516, 2013.

[2] E. Compoint and M. F. Singer. Computing Galois groups of completely reducible differential equations. *J. Symbolic Computation*, 28(4-5):473–494, 1999.

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 3, *Number* 1, *March* 2018, *pages* 55-62

Lucia Di Vizio

Direct Problem In Differential Galois Theory

Written by Alejandro Alberto Villa Isaza

1 Introduction

Galois theory of differential equations attaches an algebraic group to any linear differential system (over a differential field with an algebraically closed field of constants). Such a group provides algebraic information on the differential system. Unfortunately, the calculation of such a Galois group is quite complicated in general and we do not have an effective algorithm to accomplish this task. We present here an algorithm to calculate the Lie algebra of the Galois group, which works when the system is absolutely irreducible. The algorithm is being implemented in Maple.

1.1 A quick introduction to differential Galois theory

Let us consider the field $k := \mathbb{C}(x)$ of rational functions with complex coefficients, equipped with the derivation $\partial := \frac{d}{dx}$ acting trivially on $\mathbb{C}$ and such that $\partial(x) = 1$. We consider a linear differential system associated with the matrix A in the ring $M_n(k)$ of square matrix of order n, with entries in k:

$$[A] : \partial(Y) = AY \tag{1}$$

Definition 1 *A Picard-Vessiot extension for the differential system* (1) *is a field extension L/k, equipped with an extension of the derivation ∂, such that:*

1. *there exists $U \in \mathrm{GL}_n(L)$, verifying $\partial(U) = AU$, whose entries generate L over k;*
2. *the fields of constants L^∂ of L is $\mathbb{C}$.*

An important point in the theory is that, when the field of constants is algebraically closed, as in our case, a Picard-Vessiot extension always exists. The differential Galois group G of $\partial(y) = Ay$ is defined as

$$G := \mathrm{Gal}^\partial(L/k) := \{\varphi \text{ is a field automorphim of } L/k, \text{ commuting to } \partial\}.$$

Any automorphism $\varphi \in G$ sends U to another invertible matrix of solutions of $\partial y = Ay$, so that $U^{-1}\varphi(U) \in \mathrm{GL}_n(\mathbb{C})$. This gives a representation $G \to \mathrm{GL}_n(\mathbb{C})$ of G as a group of matrices. It turns out that G coincide with (the $\mathbb{C}$-points of) an algebraic group defined over $\mathbb{C}$. Notice that the choice of another invertible matrix of solutions leads to a conjugated representation of G.

One can define a Galois correspondence among the intermediate fields of L/k stable by ∂ and the linear algebraic subgroups of G defined over $\mathbb{C}$: to each closed algebraic subgroup H of G, one associates the field L^H of elements stable by H; to each intermediate field M of L/k, stable under ∂, one associates the group $\mathrm{Gal}^\partial(L/M)$. The relative algebraic closure $\tilde{k}$ of k in L corresponds to the connected component G_0 of the identity, so that $G_0 = \mathrm{Gal}^\partial(L/\tilde{k})$. By definition, the Lie algebra $\mathfrak{g}$ of G is the tangent space to G, or to G_0, at 1.

This is a sketch of an outline of difference Galois theory. For an extended reference, see [8].

1.2 The direct problem

The algebraic group G encodes a lot of information about the system (1), as the many applications of differential Galois theory show. For instance, the dimension of G as a variety over $\mathbb{C}$ is equal to the transcendence degree of L/k (see [8, Corollary 1.30]). Another example is the following: the connected component G_0 of G is solvable if and only if L/k is Liouvillian, that is L is obtained from k as a result of a tower of extensions of the form $K(u)/K$ such that either u is algebraic over K, or $\partial(u) \in K$ or $\partial(u)/u \in K$ (see [8, §1.5]).

The examples above show the interest of being able to calculate the differential Galois group of a differential system. The reader will also notice that, in both examples, the information needed on G can be read on G_0 or on its Lie algebra $\mathfrak{g}$.

There exist some algorithms to calculate differential Galois groups. For instance we can effectively calculate the Galois group of a differential system of rank 2, using Kovacic's algorithm [6]. There are some "theoretic" algorithms that do not make any assumption on the rank of the system: [2], [4], [7], [3]. None of them is implemented.

2 Why calculating $\mathfrak{g}$ rather than G?

2.1 Reduced forms

We denote $\bar{k}$ the algebraic closure of k. Given $A = (a_{ij}) \in M_n(\bar{k})$, we fix a basis $\alpha_1, \alpha_2, \ldots, \alpha_r \in \bar{k}$ of the $\mathbb{C}$-vector space spanned by the a_{ij}'s. Then there exist $M_1, M_2, \ldots, M_r \in M_n(\mathbb{C})$ such that $A = \sum_{h=1}^{r} \alpha_h M_h$. The matrices $M_1, M_2, \ldots, M_r$ are a Wei-Norman decomposition of A. We define $\mathrm{Lie}(A)$ as the smallest algebraic Lie sub-algebra of $M_n(\mathbb{C})$ containing $M_1, M_2, \ldots, M_r$. The Lie algebra $\mathrm{Lie}(A)$ does not depend on the choice of $\alpha_1, \alpha_2, \ldots, \alpha_r$.

Theorem 1 (Kolchin-Kovacic, [8, Corollary 1.32]) *For any differential system (1), we have the inclusion* $\mathfrak{g} \subset \mathrm{Lie}(A)$. *Moreover there exists*

$P \in GL_n(\bar{k})$ such that $P[A] := \partial(P)P^{-1} + PAP^{-1} \in \mathfrak{g}(\bar{k})$

The statement above is not very precise. Indeed, it is not $\mathfrak{g}$ which contains $P[A]$, but a conjugated algebra of $\mathfrak{g}$. In fact, we are conjugating the representation of $\mathfrak{g}$ by changing the system. However the theorem means that, up to conjugation, we have $\mathfrak{g} \subset \mathrm{Lie}(P[A])$, and hence that $\mathfrak{g} = \mathrm{Lie}(P[A])$.

Definition 2 *In the notation of the theorem above, we say that $\partial Z = P[A]Z$ is a reduced form of $\partial Y = AY$.*

2.2 Characterization of reduced forms

A differential module $\mathcal{M} = (M, \nabla)$ over k is a finite dimensional k-vector space M, say of dimension n, equipped with a $\mathbb{C}$-linear map $\nabla : M \rightarrow M$, such that $\nabla(fm) = \partial(f)m + f\nabla(m)$ for all $f \in k$ and $m \in M$. For any basis $\underline{e}$ of M over k, we have $\nabla(\underline{e}) = \underline{e}(-A)$, for some $A \in M_n(k)$. Hence an element $m \in M$, that is written as $m = \underline{e}y$, for some $y \in k^n$, verifies $\nabla(m) = 0$ if and only if $\partial(y) = Ay$. We say that $\partial(y) = Ay$ is the differential system associated to $\mathcal{M}$ in the basis $\underline{e}$. If $\underline{f}$ is another basis of M such that $\underline{e} = \underline{f}P$, then a direct calculation shows that $\nabla(\underline{f}) = \underline{f}(-P[A])$. This means that finding a reduced form is equivalent to finding a convenient basis of $\mathcal{M}$ over k.

We denote by $\mathrm{Constr}(M)$ an algebraic construction of M, i.e., a vector space obtained from M by taking duals, tensor products, direct sums and subquotients. Any such $\mathrm{Constr}(M)$ is endowed with a natural action of ∇ (see [8, §2.2] for a detailed description of the action of ∇). We denote by $\mathrm{Constr}(\mathcal{M})$ the corresponding differential module and by $\partial(y) = \mathrm{Constr}(A)y$ the system associated to $\mathrm{Constr}(\mathcal{M})$ in the basis induced by $\underline{e}$.

Notice that, if $x_0 \in \mathbb{C}$ is an ordinary point for $\partial y = Ay$, i.e., if A does not have any pole at x_0, then it is an ordinary point for any $\partial y = \mathrm{Constr}(A)y$.

Theorem 2 ([1]) *In the notation above, let x_0 be an ordinary point for $\partial y = Ay$. Then we have:*

1. *$\partial Y = AY$ is in reduced form if and only if for all algebraic construction $Constr(\mathcal{M})$ and all vectors of solution y of $\partial y = Constr(A)y$ with coefficients in k, the vector y has its coefficients in $\mathbb{C}$.*

2. *If $\partial y = AY$ is not a reduced form, then there exists a matrix $P \in GL_n(\bar{k})$ such that $\partial Z = P[A]Z$ is in reduced form and that any solution y of $\partial Y = Constr(A)Y$ with coefficients in k is sent to its value $y(x_0)$ at x_0 by the basis change associated to P.*

The theorem above says that $y(x_0)$ is solution of $\partial Y = P[\mathrm{Constr}(A)]Y$ and that $P[\mathrm{Constr}(A)] = \mathrm{Constr}(P[A])$

3 Some properties of $\mathfrak{g}$

In this paragraph, we are going to state some properties of $\mathfrak{g}$ that we use in the algorithm. The statements below are non trivial, but their proof is beyond the scope of this short exposition.

Let L be a Picard-Vessiot extension for the system $\partial y = Ay$, associated to a differential module $\mathcal{M}$, in a fixed basis. The action of ∇ extends naturally to $M \otimes_k L$, since L comes equipped with an extension of ∂. We set $V := (M \otimes_k L)^\nabla := \{m \in M \otimes_k L : \nabla(m) = 0\}$. By construction of L, V is a $\mathbb{C}$-vector space of dimension n and it is endowed with an action of G. We have a representation $G \longrightarrow \mathrm{GL}(V)$, which allows to see $\mathfrak{g}$ as a sub-Lie algebra of $\mathrm{End}(V)$, invariant under the adjoint action of G, namely $G \times \mathrm{End}(V) \longrightarrow \mathrm{End}(V)$, $(g, \psi) \mapsto g\psi g^{-1}$.

There exist two one-to-one correspondences between:

1. the subspaces of the algebraic constructions of V that are stable by the action of G,

2. the sub-differential modules of all the algebraic constructions of $\mathcal{M}$, i.e., all the sub-k-vector space of all the algebraic constructions of $\mathcal{M}$ that are stable by ∇.

They are defined by:

$$W \mapsto (W \otimes_{\mathbb{C}} L)^G, \quad (N, \nabla) \mapsto (N \otimes_k L)^{\nabla},$$

and are inverse of each other. The action of ∇ on $(W \otimes_{\mathbb{C}} L)^G$ is defined using the fact that W is a vector space of solution of a linear differential system.

As we have pointed out, the Lie algebra $\mathfrak{g}$ is a G-invariant sub-$\mathbb{C}$-vector space of $\mathrm{End}(V)$, hence $\mathfrak{g}^k := (\mathfrak{g} \otimes_{\mathbb{C}} L)^G$ is a sub-Lie algebra of $\mathrm{End}(\mathcal{M}) \cong \mathcal{M} \otimes \mathcal{M}^*$.[1]

The algorithm that we are presenting here, is articulated in two parts: first it calculates $\mathfrak{g}^k$ and then deduces $\mathfrak{g}$ from $\mathfrak{g}^k$, constructing the matrix P mentioned in Theorem 2. Indeed, $\mathfrak{g}^k$ is a sub-module of $\mathcal{M} \otimes_k \mathcal{M}^*$, stable by ∇. Hence it is generated by some matrices $M_i(x) \in M_n(k)$, for $i = 1, \ldots, s$. Then $\mathfrak{g}$ will be generated by their values $M_i(x_0)$ in an ordinary point x_0.

4 The algorithm

The algorithm works under the following assumption: the differential module $\mathcal{M}$ is absolutely irreducible, that is, the differential module $\mathcal{M} \otimes_k \bar{k}$ does not have any non trivial sub-differential module. This ensures that $\mathfrak{g}$ acts irreducibly on V and that $\mathcal{M} \otimes_k \mathcal{M}^*$ is a direct sum of irreducible differential modules.

We also make the more innocent assumption, to whom one can always reduce, that $\mathfrak{g}$ is contained in $\mathfrak{sl}_n(\mathbb{C})$, which implies that $\mathfrak{g}$ is semi-simple.

The algorithm proceeds as follow:

[1] The Lie algebra $\mathfrak{g}^k$ is nothing else than the Lie algebra introduced by N. Katz in [5].

1. One decomposes $\mathcal{M} \otimes_k \mathcal{M}^*$ using the properties of the eigenring (see [8, Proposition 2.40]). This boils down to finding the rational solutions of a differential system of rank n^4, which increases considerably the complexity of the algorithm. Fortunately, there are some canonical decompositions of $\mathcal{M} \otimes_k \mathcal{M}^*$ that allow, for instance, to consider two differential systems of rank $(n^2-1)n^2/2$ and $(n^2-1)(n^2-2)/2$, rather than of rank n^4. In spite of the appearances, it is quite a gain since for $n = 3$ one has to solve two systems of rank 36 and 28, which is already much faster than solving a system of rank 81.

2. One has to select the pieces of the decomposition of $\mathcal{M} \otimes_k \mathcal{M}^*$ containing $\mathfrak{g}^k$. This is done systematically, testing all the proper submodules of $\mathcal{M} \otimes_k \mathcal{M}^*$. So, the algorithm selects a maximal submodule $\mathfrak{g}^{guess}$ and it goes to the next step to test it.

3. The test consists in trying to find the matrix P. There are two possibilities:

    a) It can find P: it means that $\mathfrak{g}^k \subset \mathfrak{g}^{guess}$. Then it goes back to step 2 and tests of all the proper maximal submodules of $\mathfrak{g}^{guess}$ to see if it has to replace $\mathfrak{g}^{guess}$ by a smaller candidate or if we have found $\mathfrak{g}^k$ and P, and therefore $\mathfrak{g}$.

    b) It cannot find P: it means that $\mathfrak{g}^k \not\subset \mathfrak{g}^{guess}$, so it goes back to step 2 and picks another candidate.

References

[1] A. Aparicio Monforte, E. Compoint, and J.-A. Weil. A characterization of reduced forms of linear differential systems. *Journal of Pure and Applied Algebra*, 217(8):1504–1516, 2013.

[2] E. Compoint and M. F. Singer. Computing Galois groups of completely reducible differential equations. *J. Symbolic Computation*, 28(4-5):473–494, 1999.

[3] R. Feng. Hrushovski's algorithm for computing the Galois group of a linear differential equation. *Advances in Applied Mathematics*, 65:1 – 37, 2015.

[4] E. Hrushovski. Computing the Galois group of a linear differential equation. In *Differential Galois theory (Bedlewo, 2001)*, volume 58 of *Banach Center Publ.*, pages 97–138. Polish Acad. Sci., Warsaw, 2002.

[5] N. M. Katz. A conjecture in the arithmetic theory of differential equations. *Bull. Soc. Math. France*, 110(2):203–239, 1982.

[6] J. J. Kovacic. An algorithm for solving second order linear homogeneous differential equations. *J. Symbolic Comput.*, 2(1):3–43, 1986.

[7] J. van der Hoeven. Around the numeric-symbolic computation of differential Galois groups. *J. Symbolic Comput.*, 42(1-2):236–264, 2007.

[8] M. van der Put and M. F. Singer. *Galois theory of linear differential equations*, volume 328 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 2003.

Alejandro Alberto Villa Isaza
Dipartimento Di Matematica e Fisica
Università Degli Studi Di Roma Tre
Largo San Leonardo Murialdo 1
00145, Rome, Italy.
email: `villaisaza@mat.uniroma3.it`

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 3, Number 1, March 2018, pages 63-68

Fernando Rodriguez Villegas

Hypergeometric motives: Hodge numbers and supercongruences

Editorial committee

Consider the Dwork family of quintic threefolds in $\mathbb{P}^4$

$$X_\psi : x_1 + x_2 + x_3 + x_4 + x_5 - 5\psi x_1 x_2 x_3 x_4 x_5 = 0 \tag{1}$$

where $\psi \in \mathbb{C}$ is a parameter. The non singular member of the family are Calabi-Yau varieties. Recall that a complex connected, compact Kähler manifold X is called a Calabi-Yau variety if

(CY1) the canonical bundle is trivial

(CY2) there are no p-holomorphic forms for $p \neq 0, n$, where n is the complex dimension of X.

Smooth hypersurfaces of degree $n + 1$ in a n-dimensional projective space are Calabi-Yau as consequence of adjunction and the Lefschetz theorem. Elliptic curve and $K3$ surfaces are the only examples of Calabi-Yau variety in dimension 1 and 2. It is not difficult to show that if ψ is not a fifth root unity then X_ψ is smooth and hence is a Calabi-Yau threefold. Let

$$P_\psi(x_1, \ldots, x_5) = x_1 + x_2 + x_3 + x_4 + x_5 - 5\psi x_1 x_2 x_3 x_4 x_5$$

The Hodge diamond of X_ψ looks a follows

$$\begin{array}{ccccccc}
 & & & 1 & & & \\
 & & 0 & & 0 & & \\
 & 0 & & 1 & & 0 & \\
1 & & 101 & & 101 & & 1 \\
 & 0 & & 1 & & 0 & \\
 & & 0 & & 0 & & \\
 & & & 1 & & &
\end{array}$$

In particular $H^1(X_\psi, \mathbb{C}) = H^5(X_\psi, \mathbb{C}) = 0$ and $H^0(X_\psi, \mathbb{C})$, $H^2(X_\psi, \mathbb{C})$, and $H^4(X_\psi, \mathbb{C})$ are one dimensional.

Suppose that $\psi \in \mathbb{Q}$ then we can reduce modulo a prime p primes not dividing its denominator; assume $p > 5$.For varieties over finite fields an important quantity is the number of points

$$N_p(X_\psi) = \# \left\{ P \in \mathbb{P}^4(\mathbb{F}_p) \mid P \in X_\psi \right\}.$$

Then if we set

$$A_p = \sum_{(x_1, \ldots, x_5) \in \mathbb{F}_p^5} \left(1 - P_\psi(x_1, \ldots, x_5)^{p-1} \right) \tag{2}$$

we have that

$$A_p \equiv 1 - (p-1) N_p(X_\psi) \bmod p$$

hence

$$A_p - 1 \equiv N_p(X_\psi) \bmod p.$$

A prime is called a good prime for X_ψ if the reduction of $X_\psi bmodp$ is non singular.

Next we want to introduce the generalized hypergeometric functions. Let r and s be integers, and $\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s$ be rational number with all the $-\beta_i$ different from non-negative integers. The generalized hypergeometric function is defined as the series

$${}_rF_s \left(\begin{matrix} \alpha_1 & \cdots & \alpha_r \\ \beta_1 & \cdots & \beta_s \end{matrix} \middle| t \right) == \sum_{k=0}^{\infty} \frac{(\alpha_1)_k \ \ldots \ (\alpha_r)_k}{(\beta_1)_k \ \ldots \ (\beta_s)_k} \frac{t^k}{k!}$$

where $(x)_k = x(x+1)\cdots(x+k-1)$. We want to compute $A_p \bmod p$ in terms of truncated generalized hypergeometric function. First of all recall that

$$\sum_{x\in\mathbb{F}_p^*} x^a = \begin{cases} p-1 & \text{if } a \equiv 0 \bmod p \\ 0 & \text{if } a \not\equiv 0 \bmod p \end{cases}$$

Expanding the polynomial in (2) and using the above relation it is not hard to show that:

$$A_p \equiv \sum_{m=0}^{\lfloor p/5 \rfloor} \frac{(5m)!}{m!^5} \left(\frac{t}{5^5}\right)^m \bmod p$$

where $t = \psi^{-5}$. See [1, p. 38] for more details. On the right hand side we have the truncatation of the generalized hypergeometric function:

$$\sum_{m=0}^{\infty} \frac{(5m)!}{m!^5} \left(\frac{t}{5^5}\right)^m = {}_4F_3\left(\begin{matrix} \frac{1}{5} & \frac{2}{5} & \frac{3}{5} & \frac{4}{5} \\ 1 & 1 & 1 & \end{matrix} \middle| t\right)$$

Another important aspect of this theory are the periods of X_ψ. Recall that, roughly speaking, a period on a k-dimensional variety (defined over $\overline{\mathbb{Q}}$) is the value of the integral along a k-cycle (with some boundary condition) of a k-differential form (for more about periods and their relevance in arithmetic geometry see [2]). Note that $(CY1)$ implies that X_ψ admits a nowhere-vanishing holomorphic 3-form ω_ψ, unique up to scalar multiplication, which can be defined as:

$$\mathrm{Res}_{X_\psi}\left(\frac{\sum_{i=1}^5 (-1)^i x_i dx_1 \wedge \cdots \wedge \widehat{dx_i} \wedge \cdots \wedge dx_5}{x_1+x_2+x_3+x_4+x_5-5\psi x_1x_2x_3x_4x_5}\right)$$

Therefore the periods of X_ψ, are the values

$$\int_\gamma \omega_\psi$$

where γ is a 3-cycle. Moreover the dimension of $H^3(X_\psi, \mathbb{C}) = 204$ which means there are 204 periods of ω_ψ.

Consider the abelian subgroup of automorphisms

$$A := \{(\zeta_1, ..., \zeta_5) | \zeta_i^5 = 1, \zeta_1 \cdots \zeta_5 = 1\},$$

acting by $x_i \mapsto \zeta_i x_i$ and let V_ψ be the subspace of $H^3(X_\psi, \mathbb{C})$ fixed by A. It can be shown that the dimension of V_ψ is 4.

There is also another way to compute the number of points of X_ψ mod p which is done via the Frobenius endomorphism and goes as follows: For a good prime p, let Frob_p denote the Frobenius morphism on X_ψ induced by the p-th power map $x \longrightarrow x^p$. Let ℓ be a prime different from p. Then the induced operator Frob_p^* acts on the ℓ adic étale cohomology groups $H^i_{et}(X_\psi, \mathbb{Q}_\ell)$. Let

$$P_{p,i}(T) := \det(1 - T\,\mathrm{Frob}_p^* \,|H^i_{et}(X_\psi, \mathbb{Q}_\ell)$$

be the characteristic polynomial of the endomorphism Frob_p^* on the étale ℓ-adic cohomology group, where T is an indeterminate. By the Lefschetz fixed point formula we have that

$$N_p(X_\psi) = \#\,\mathrm{Fix}(\mathrm{Frob}_p) = \sum_i (-1)^i\,\mathrm{Tr}(\mathrm{Frob}_p^* \,|H^i_{et}(X_\psi, \mathbb{Q}_\ell)).$$

Recall that we set $t = \psi^{-5}$. If $t \longrightarrow 1$ (i.e. $\psi \longrightarrow$ a root of unitiy), then dimension of V_ψ^I the fixed part of V_ψ under the action of the inertia group has dimension 3 and split as the direct sum of L and A, where L has dimension 1 and A has dimension 2 and is associated to a modular form f of weight 4 and level 125 (as proven by C. Schoen in [6]). Moreover

$$\text{Trace of Frobenius on } V = \left(\frac{p}{5}\right) p + a_p,$$

where a_p is the $p - th$ coefficent of the modular form found by Schoen and $\left(\frac{p}{5}\right)$ is the Legendre symbol. It follows that

$$\sum_{m=0}^{\lfloor p/5 \rfloor} \frac{(5m)!}{m!^5} 5^{-5m} \equiv a_p \bmod p$$

Experimentally this congruence actually happens mod p^3 (but only for $t = 1$), which is rather surprising, and this fact has been given the name of *supercongruence*. One can find a few other examples of this kind in [5] (for a recent proof see [3]).

Together with D. Roberts we have found a conjectural explanation of this supercongruence phenomenon tying it to the gap in the Hodge numbers of the limiting motive at $t = 1$. In our case this motive is that of the modular form f, which being of weight 4 has Hodge numbers $(1, 0, 0, 1)$. The gap of 3 between the non-zero Hodge numbers should explain the observed supercongruence to the power p^3. For more details see [4].

References

[1] P. Candelas, X. de la Ossa and F. Rodriguez-Villegas, *Calabi-Yau manifolds over Finite Fields I*, pp 76, hep-th/0012233

[2] M. Kontsevich and D. Zagier, *Periods.* In Mathematics Unlimited 2001 and Beyond. Springer, pages 771?808, 2001.

[3] L. Long, F.-T. Tu, N. Yui, W. Zudilin *Supercongruences for rigid hypergeometric Calabi–Yau threefolds* https://arxiv.org/abs/1705.01663

[4] D. Roberts and F. Rodriguez Villegas, *Hypergeometric supercongruences* https://www.matrix-inst.org.au/2017-matrix-annals

[5] F. Rodriguez Villegas *Hypergeometric families of Calabi-Yau manifolds* Calabi-Yau varieties and mirror symmetry (Toronto, ON, 2001), 223–231, Fields Inst. Commun., 38, Amer. Math. Soc., Providence, RI, 2003.

[6] C. Schoen, *On the geometry of a special determinantal hypersurface associated to the Mumford-Horrocks bundle*, J. Reine Angew. Math. 364 (1986), 85-111.