Proceedings of the 5th mini symposium of the Roman Number Theory Association

Università Roma Tre

April 10th-12th, 2019

IF Press srl - Roma, Italy
info@if-press.com - www.if-press.com

ISBN 978-88-6788-267-0

Contents

Foreword v

Part I - The Scriba Project

Cécile Armana
Sturm bounds for automorphic forms of Drinfeld type over function fields
Dario Antolini 1

Yuri Bilu
Singular units do not exist
Francesco Campagna 9

Peter Stevenhagen
Elliptic curves and primes of cyclic reduction
Raiza Corpuz 17

Shabnam Akhtari
Lower bounds for the Mahler measures of polynomials that are sum of a bounded number of monomials
Mahadi Ddamulira 23

Andrew Granville
Multiplicative functions in short intervals and arithmetic progressions
Alessandro Fazzari 33

David Kohel
Orienting Supersingular Isogeny Graphs
Boris Fouotsa Tako 41

Pär Kurlberg
Prime and Möbius correlations for very short intervals in $\mathbb{F}_p[X]$.
Oussama Rayen Hamza 51

David Masser
On Siegel's Lemma
Guido Lido 59

Florian Luca
Coordinates of Pell equations in various sequences
Andam Mustafa 67

Sara Checcoli
Fields of algebraic numbers with bounded local degrees and their Galois groups
Lorenzo Pagani 81

Marusia Rebolledo
Abelian varieties with large Galois image
Mohamadou Sall 89

Pieter Moree
Irregular behaviour of class numbers and Euler-Kronecker constants of cyclotomic fields: the log log log devil at play
Pietro Sgobba 99

Part II - Contributed talks

Classification of Number Fields with Minimum Discriminant
Francesco Battistoni 107

Summary of results on Algebraic Geometry codes over abelian surfaces containing no absolutely irreducible curves of low genus
Yves Aubry, Elena Berardini, Fabien Herbaut & Marc Perret 109

On zero-sum subsequences in a finite abelian p-group of length not exceeding a given number
Bidisha Roy and R. Thangadurai 111

Kummer Theory for Number Fields
Antonella Perucca, Pietro Sgobba, Sebastiano Tronto 113

Statistics of moduli space of vector bundles
Sampa Dey 115

Approximations by Signed Harmonic Sums and the Thue–Morse Sequence
Sandro Bettin, Giuseppe Molteni, Carlo Sanna 117

Multidimensional p-adic continued fractions
Nadir Murru, Lea Terracini 119

Foreword

This volume contains the proceedings of the Fifth mini symposium of the Roman Number Theory Association. The conference was held on April 10-12, 2019 at the Università degli Studi Roma Tre. As well as for the fourth Symposium, the duration was of three days and we also hosted, as a satellite conference, the 13th PARI/GP Atelier.

As organizers of the symposium, and promoters of the association, we would like to thank the main speakers, as well than the participants who presented a contributed talk, for the high scientific contribution offered, and the "scribas" who wrote these notes. We also thank the funding bodies, and among them the Università Europea di Roma and the Università Roma Tre for their support.

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 organizing 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 topics 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, the Second and Third Mini Symposium, was slightly peculiar. 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 main 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 years, the Roman Number Theory Association has been involved in many different activities, even if, clearly, our program was badly affected by the pandemic. We have been forced to postpone the Sixth mini Symposium of the association any many conferences and research schools. We are now restarting our activities and trying to make up for lost time. Indeed, the Association collaborated in various ways to several events, namely:

- *Leuca2022, Celebrating Claude Levesque's, Damien Roy's and Michel Waldschmidt's birthdays* to be held on May 16-21, 2022, Marina di San Gregorio, Pat (Lecce), Italy;
- *13th Atelier PARI/GP*, Universit Roma Tre, April 8-9, 2019;
- *The Twelfth International Conference on Science and Mathematics Education in Developing Countries*, The National University of Laos, Laos, held in November 2019;

Another very important engagement of the association was in the participation in some CIMPA schools. The main idea of CIMPA Schools, supported by UNESCO, perfectly espouses one of the central aspects of RNTA, namely organisation and funding of scientific and educational activities in Developing Countries. The most recent (or future) CIMPA school we are involved in are the following:

- CIMPA research school on *Algebra, arithmetic and applications*, Institut de Mathématiques et de Sciences Physiques, Dangbo, Bénin June, 12-24 2022

- CIMPA research school on *Introduction to Galois representations and modular forms and their computational aspects* , University of the Philippines Diliman January 10-21, 2022

- WAMS School *Topics in commutative algebra* , University of Sulaimani, Sulaimani, Kurdistan Region, Iraq , Spring 2022

- WAMS School *Topics in algebraic number theory*, Salahaddin University, Erbil, Kurdistan Region, Iraq, Spring 2022

- Senegal EMA school on *Introduction to Number Theory, Cryptography and related courses*, African Institute of Mathematical Sciences (M'bour) Senegal September 6 - 19, 2021

- CIMPA research school on *Group Actions in Arithmetic and Geometry*, Universitas Gadjah Mada Yogyakarta, Indonesia February 17-28, 2020

- CIMPA research school on *Algebraic Geometry, Number Theory and Applications in Cryptography and Robot kinematics*, AIMS-Cameroon, Limbe. July 2-13, 2019

- WAMS research school on *Introductory topics in Number Theory and differential Geometry*, King Khalid University, Abha, Saudi Arabia, June 16-23, 2019

- CIMPA research school on *Elliptic curves: arithmetic and computation*. Universidad de la Repblica, Montevideo, Uruguay, February 11 - 22, 2019.

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.

During the years, the RNTA, collaborates with many institutions, here the list of our main partners:

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.

Fabrizio Barroero, Dipartimento di Matematica e Fisica, Università Roma Tre
email: barroero@mat.uniroma3.it

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

Part I
The Scriba Project

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 5, *Number* 1, *March* 2022, *pages* 1-7

Cécile Armana

Sturm bounds for automorphic forms of Drinfeld type over function fields

Written by Dario Antolini

The aim of this proceeding is to explain a theorem of Armana and Wei about the Sturm bound for harmonic cochains. Since harmonic cochains are "characteristic-p analogue" of modular forms, we first introduce the Sturm bound in this classical setting.

As many introductory courses teach, a modular form f of weight an integer number k for the subgroup $\Gamma_0(N)$, denoted $f \in M_k(\Gamma_0(N))$, has a Fourier expansion of the form:

$$f(z) = \sum_{n=0}^{+\infty} c_n(f) q^n,$$

where $q := e^{2i\pi z}$ for $z \in \mathbb{H} := \{z \in \mathbb{C} : \ \mathrm{Im}(z) > 0\}$.

Since the sum is infinite, one can wonder if there exists some bound on the number of coefficients needed to determine such modular form, and whenever the answer is positive to find a good estimate.

Sturm gave a positive answer to the above question ([4, Theorem 2]).

Theorem 1 *Let* $f \in M_k(\Gamma_0(N))$.
If $c_n(f) = 0$ *for any* $0 \leq n \leq \frac{k}{12}[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)]$, *then* $f \equiv 0$.

Proof. Let us sketch some elements of the proof.

1. Case $N = 1$: for $f \in M_k(\mathrm{SL}_2(\mathbb{Z}))$, $f \neq 0$, use the valence (or $\frac{k}{12}$-) formula (e.g., see [3, Ch.VIII, Thm.3]):

$$v_\infty(f) + \sum_{P \in \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}} \frac{v_P(f)}{e_P} = \frac{k}{12},$$

   where $v_P(f)$ is the order of f at P, $v_\infty(f)$ is the order of its Fourier expansion at $q = 0$ and e_P are certain positive integers.

   Thus, $v_\infty(f) \leq k/12$.

2. Case $N > 1$: write $\mathrm{SL}_2(\mathbb{Z}) = \bigcup_{i=1}^{M} \Gamma_0(N) y_i$, where $M = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)]$, put $\tilde{f} = \prod_{i=1}^{M} f_{|k[y_i]} \in \mathrm{M}_{Mk}(\mathrm{SL}_2(\mathbb{Z}))$ and apply point 1.

□

Remark 2 *The inequality is sharp, as we can check in the full level case* $\Gamma_0(1) = \mathrm{SL}_2(\mathbb{Z})$ *and weight* $k = 12$*: there is just one non-zero normalized cuspidal modular form, the so-called discriminant* Δ*.*

For whom interested in computer implementations, there are some commands for PARI/GP and Sage which compute the bound for any $f \in M_k(\Gamma_0(N))$:

- `PARI/GP:` `mfsturm([N,k])`
- `Sage:` `ModularForms(Gamma0(N),k).sturm_bound()`

As a corollary, we get also a bound for the generators of the Hecke algebra $\mathbb{T}_k(\Gamma_0(N)) := \mathbb{C}[T_n \mid n \geq 1] \subset \mathrm{End}(S_k(\Gamma_0(N)))$.

Corollary 3 *The Hecke algebra* $\mathbb{T}_k(\Gamma_0(N))$ *is generated, as* $\mathbb{C}$*-vector space, by all the Hecke operators* T_n *with* $1 \leq n \leq \frac{k}{12}[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)]$.

The idea of the proof is to use the perfect $\mathbb{C}$-pairing

$$S_k(\Gamma_0(N)) \times \mathbb{T}_k(\Gamma_0(N)) \to \mathbb{C}, \quad (f, T) \mapsto c_1(Tf).$$

Now, we move our attention to the function field (or Drinfeld) setting with positive characteristic $p > 0$.
Let q be a power of p and replace the integers $\mathbb{Z}$ inside its fraction field $\mathbb{Q}$ by the ring $A := \mathbb{F}_q[t]$ inside the field $K := \mathbb{F}_q(t)$; hence, consider the completion $K_\infty := \mathbb{F}_q(\!(1/t)\!)$ at the infinity place $1/t$ and its algebraic closure $\overline{K_\infty}$. Since the extension $\overline{K_\infty}/K_\infty$ has infinite degree, the latter is no more complete, but still taking its completion C_∞ it remains algebraically closed.

For an element $N \in A$, also define:

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(A) \mid c \equiv 0 \pmod{N} \right\}.$$

In this world, one can generalize the notion of modular forms in two ways: via Drinfeld modular forms (case of equal characteristic with values in C_∞) and via harmonic cochains (case of mixed characteristic with values in $\mathbb{C}$). In this exposé, we will use the second ones.

Before defining them, we need to introduce the Bruhat–Tits tree $\mathcal{T}$ of $\mathrm{PGL}_2(K_\infty)$, a combinatorial version of the Poincaré upper-half plane.
If we denote by $\mathrm{GL}_2(O_\infty)$ (resp., by I_∞) the maximal compact subgroup (resp., the Iwahori subgroup) of $\mathrm{GL}_2(K_\infty)$, where O_∞ is the ring of integers of K_∞, define an oriented graph $\mathcal{T}$ as follows:

- vertices: $V(\mathcal{T}) = \mathrm{GL}_2(K_\infty)/K_\infty^\times \cdot \mathrm{GL}_2(O_\infty)$;
- edges: $E(\mathcal{T}) = \mathrm{GL}_2(K_\infty)/K_\infty^\times \cdot I_\infty$;
- finallly, the orientation of the edges is given by the canonical map $o\colon E(\mathcal{T}) \to V(\mathcal{T})$ which associates to each edge its origin.

It is a result of Serre ([2, Ch.II, Sec.1]) that $\mathcal{T}$ is indeed a $(q+1)-$regular tree provided with a transitive action of $G(K_\infty)$ and an involution on

the set of vertices $E(\mathcal{T})$ which takes an oriented edge e to its opposite $\bar{e}$.

A *harmonic cochain* on $\mathcal{T}$ of level $\Gamma_0(N)$ is a function $f\colon E(\mathcal{T}) \to \mathbb{C}$ satisfying:

1. (alternate) $\forall e \in E(\mathcal{T})$, $f(e) + f(\bar{e}) = 0$;
2. (harmonic) $\forall v \in V(\mathcal{T})$, $\sum_{o(e)=v} f(e) = 0$;
3. ($\Gamma_0(N)$−left invariance) $\forall \gamma \in \Gamma_0(N)$, $\forall e \in E(\mathcal{T})$, $f(\gamma e) = f(e)$.

Moreover, we say that f is *cuspidal* if f is finitely supported on $E(\Gamma_0(N)\backslash\mathcal{T})$. The space of harmonic cochains (resp., cuspidal) of level $\Gamma_0(N)$ is a $\mathbb{C}$-vector space denoted by $H(\Gamma_0(N))$ (resp., $H_c(\Gamma_0(N))$), and it is finite dimensional as in the classical case.

For commodity of the discussion, let's fix a uniformiser $\pi = 1/t$ of $O_\infty = \mathbb{F}_q[\![1/t]\!]$ and a set of representatives for the set of positive edges $E^+(\mathcal{T})$:

$$\left\{ \begin{pmatrix} \pi^r & u \\ 0 & 1 \end{pmatrix} \mid r \in \mathbb{Z}, u \in K_\infty/\pi^{-r}O_\infty \right\}.$$

The harmonic cochains admit a Fourier expansion similar as in the classical case: for $f \in H(\Gamma_0(N))$, $r \in \mathbb{Z}$ and $u \in K_\infty$, we can write

$$f\begin{pmatrix} \pi^r & u \\ 0 & 1 \end{pmatrix} = q^{-r+2}\left(c_o(f) + \sum_{\substack{\text{monic } m \in A \\ \deg m \leq r-2}} c_m(f)\,\psi(mu) \right) \tag{1}$$

where $c_m(f) = q^{\deg m}\int_{A\backslash K_\infty} f\begin{pmatrix} \pi^{\deg m+2} & u \\ 0 & 1 \end{pmatrix}\psi(-mu)\,du$ and $\psi\colon K_\infty \to \mathbb{C}^\times$ is an additive character.

Therefore, one can ask for a good Sturm bound for harmonic cochains, namely to find a (hopefully sharp) integer B for which it is enough to consider the coefficients $c_m(f)$ with $\deg m \leq B$. In general, one can hope to adopt the proofs of the classical case in this setting, but this is

not the case: we don't have either a valence formula and a Riemann–Roch theorem for finite graphs as good as the classical modular curves. However, what we have is a very good knowledge of the quotient graph $\Gamma_0(N)\backslash\mathcal{T}$ (a combinatorial analogue of the modular curve, see e.g. [2] and [1]).

In fact, the approach of Armana and Wei is to find a set S of matrices of the form $g = \begin{pmatrix} \pi^r & u \\ 0 & 1 \end{pmatrix}$ with $0 \leq r \leq B$ (for some B) such that any harmonic cochain $f \in H_c(\Gamma_0(N))$ is uniquely determined by its values on the classes $\{[g]\}_{g\in S}$ in $E(\mathcal{T})$. Thus, from the Fourier expansion (1) one get the Sturm bound: $\deg m \leq B - 2$.

After the work of Gekeler–Nonnengardt, one can obtain the set $S = \left\{ \begin{pmatrix} \pi^r & * \\ 0 & 1 \end{pmatrix} \mid 0 \leq r \leq 3\deg N - 3 \right\}$, because it trivially contains the support of cochain f. Hence, we get a first Sturm bound:

$$\deg m \leq 3\deg N - 5.$$

The result of Armana and Wei improves this estimate.

Theorem 4 (Armana-Wei) *Let $f \in H_c(\Gamma_0(N))$.*
Assume that $c_m(f) = 0$ for any monic $m \in A$ and:

1. $\deg m \leq 2\deg N - 4$ *if N is arbitrary;*
2. $\deg m \leq \deg N - 2$ *if N is squarefree and f is a newform;*
3. $\deg m \leq \deg N - 2$ *if $N = P^l$ with P irreducible;*
4. $\deg m \leq \deg N - 1$ *if $N = P_1^{l_1} \cdots P_s^{l_s}$ with $P_1, \ldots, P_s$ irreducible and $s \leq q$.*

Then $f \equiv 0$.

The main tools of the proof are harmonicity, Atkin–Lehner involutions, Gekeler–Nonnengardt results and pigeon-hole principle.

Remark 5 *The bounds (2), (3) and (4) are optimal.*
For the general bound, the expected optimal bound is $\deg N + cst$.

As in the classical case, we get for free a Sturm bound for the Hecke operators.

Define $\mathbb{T}(\Gamma_0(N)) = \mathbb{C}[T_m \mid m \text{ monic in } A] \subset \mathrm{End}(H_c(\Gamma_0(N)))$. Using the perfect $\mathbb{C}$-pairing

$$H_c(\Gamma_0(N)) \times \mathbb{T}(\Gamma_0(N)) \to \mathbb{C}, \quad (f, T) \mapsto c_1(Tf),$$

we get:

Corollary 6 *The Hecke algebra* $\mathbb{T}(\Gamma_0(N))$ *is generated as* $\mathbb{C}$*-vector space by the Hecke operators* T_m *with* $m \in A$ *monic and:*

1. $\deg m \leq 2 \deg N - 4$ *if* N *is arbitrary;*
2. $\deg m \leq \deg N - 2$ *if* $N = P^l$ *and* P *irreducible;*
3. $\deg m \leq \deg N - 1$ *if* $N = P_1^{l_1} \cdots P_s^{l_s}$ *with* $P_1, \ldots, P_s$ *irreducible and* $s \leq q$.

References

[1] Gekeler, Ernst-Ulrich, and Udo Nonnengardt, *Fundamental domains of some arithmetic groups over function fields*, International Journal of Mathematics 6.5 (1995): 689-708.

[2] Serre, Jean-Pierre, *Trees*. 1980.

[3] Serre, Jean-Pierre, *A course in arithmetic*. Vol. 7. Springer Science & Business Media, 2012.

[4] Sturm, Jacob, *On the congruence of modular forms*. In: *Number theory: A Seminar held at the Graduate School and University Center of the City University of New York 1984-85*, 275-280, Springer Berlin Heidelberg, 1987.

Dario Antolini
Department of Mathematics
Università degli Studi di Roma "Tor Vergata"
Via della Ricerca Scientifica, 1
00133 – Roma (Italy).
email: antolini@mat.uniroma2.it - dario.ant27@gmail.com

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 5, *Number* 1, *March* 2020, *pages* 9-15

Yuri Bilu

Singular units do not exist

Written by Francesco Campagna

1 What are singular moduli?

A **singular modulus** is the j-invariant of an elliptic curve defined over $\mathbb{C}$ with complex multiplication. Equivalentely, if $\mathbb{H}$ denotes the Poincaré half plane and $j : \mathbb{H} \to \mathbb{C}$ is the usual modular j-function with q-expansion:

$$j(z) = \frac{1}{q} + 744 + 196884q + \dots \qquad q = e^{2\pi i z},$$

then a singular modulus is a value $j(\tau)$, with $\tau \in \mathbb{H}$ imaginary quadratic. Notice that every imaginary quadratic $\tau \in \mathbb{H}$ defines a lattice $[1, \tau] = \mathbb{Z} + \mathbb{Z}\tau \subseteq \mathbb{C}$ which is homothetic to a proper fractional ideal of a unique order $\mathcal{O}_\tau$ in an imaginary quadratic field. Then the elliptic curve associated to the quotient $\mathbb{C}/[1, \tau]$ has complex multiplication precisely by the order $\mathcal{O}_\tau$.

Fix $\tau \in \mathbb{H}$ imaginary quadratic and let

$$f(T) = aT^2 - bT + c \in \mathbb{Z}[T]$$

be the minimal polynomial of τ over $\mathbb{Z}$. We define the **discriminant** of the singular modulus $x := j(\tau)$ as

$$\Delta_x := \operatorname{disc} f(T) = b^2 - 4ac.$$

This is also equal to the discriminant of the order O_τ defined above. It is clear from the definition that the discriminant of a singular modulus is a negative integer congruent to 0 or 1 modulo 4. On the other hand, for any negative integer $\Delta \equiv 0, 1 \bmod 4$ there exists a unique quadratic order O_Δ of discriminant Δ; if we view the proper fractional ideals of this order as lattices in $\mathbb{C}$ and we compute their j-invariants, we obtain precisely all the singular moduli of discriminant Δ. It is clear that two proper fractional ideals are in the same ideal class if and only if they are homothetic as lattices in $\mathbb{C}$. Hence all the proper ideals in the same ideal class will give rise to the same singular modulus. We conclude that for any negative integer $\Delta \equiv 0, 1 \bmod 4$ there are precisely $C(\Delta)$ singular moduli of discriminant Δ, where $C(\Delta)$ is the class number of the unique order of discriminant Δ.

However, one could prove even more: singular moduli of discriminant Δ are algebraic integers of degree $C(\Delta)$ and they form a full Galois orbit over $\mathbb{Q}$. This fact will be heavily used in what follows.

2 Finitness of singular units: a proof by Habegger

A well-known theorem of André (see [1]) asserts that, apart from some "obvious" exceptions, equations of the form $f(x, y) = 0$ for $f \in \mathbb{C}[x, y]$ have finitely many solutions (j_1, j_2) with j_1 and j_2 both singular moduli. However, the proof of this result is not effective and in recent years many efforts have been done in order to obtain effective results on special families of equations. In particular in [3] it is shown that the equation $xy = 1$ has no solution in singular moduli. Motivated by this result, D. Masser asked whether it is possible that a singular modulus can be a unit in the ring of algebraic integers. Such a singular modulus will be called a singular unit.

A first answer to this question has been given by P. Habegger in [7], where it is proved the following

Theorem 2.1 *There exist at most finitely many singular units.*

In what follows we will try to give an overview of the proof of this result.

The idea is, given a singular unit x of discriminant Δ, to provide an upper and a lower bound for its Weil height $h(x)$ which contradict each other when $|\Delta|$ is sufficently large. From some results of Colmez and Nakkajima-Taguchi on the stable Faltings height of a CM elliptic curve (see [5] and [9] respectively) one gets the lower bound

$$h(x) \geq c_1 \log|\Delta| - c_2 \qquad c_1, c_2 > 0. \tag{1}$$

As far as the upper bound is concerned, the author proceeds as follows: since x^{-1} is an algebraic integer, the finite places do not contribute to the computation of its Weil height. Hence we can write:

$$h(x) = h(x^{-1}) = \frac{1}{C(\Delta)} \sum_{1 \leq k \leq C(\Delta)} \log^+ |x_k^{-1}|. \tag{2}$$

where, for every $k = 1, ..., C(\Delta)$, the x_k are the Galois conjugates of the singular modulus x. We have then to control the conjugates that are small in absolute value. Fix $0 < \varepsilon < 1$ and let $\mathcal{F}$ be the usual fundamental domain for the action of $\mathrm{SL}_2(\mathbb{Z})$ on the Poincaré half plane. Note that for every $k = 1, ..., C(\Delta)$ there is a unique $\tau_k \in \mathcal{F}$ for which $x_k = j(\tau_k)$. Define the "cat's ears" as

$$U_\varepsilon := \{z \in \mathcal{F} : \min\{|z - \zeta_6|, |z - \zeta_3|\} < \varepsilon\}$$

where $\zeta_6 = e^{\frac{2\pi i}{6}}$ and $\zeta_3 = e^{\frac{2\pi i}{3}}$. Notice that the $\tau_k \in U_\varepsilon$ give rise to singular moduli x_k of small absolute value since ζ_6 and ζ_3 are zeros of the j-function. By splitting the sum in formula (2) as

$$h(x) = \frac{1}{C(\Delta)} \sum_{\tau_k \in U_\varepsilon} \log^+ |x_k^{-1}| + \frac{1}{C(\Delta)} \sum_{\tau_k \notin U_\varepsilon} \log^+ |x_k^{-1}|$$

and by estimating separately the two sums, the author gets

$$h(x) \leq \frac{C_\varepsilon(\Delta)}{C(\Delta)} c_3 \log|\Delta| + 3 \log \varepsilon^{-1} + c_4 \tag{3}$$

where $C_\varepsilon(\Delta) = \#(\{\tau_1, ..., \tau_k\} \cap U_\varepsilon)$ and c_3, c_4 are positive real constants. Hence, in order to conclude, one has to bound the quantity $\frac{C_\varepsilon(\Delta)}{C(\Delta)}$. Here Habegger uses Duke-Clozel-Ullmo equidistribution (see [4] and [6]) to prove that, for $|\Delta|$ sufficiently large, one has

$$\frac{C_\varepsilon(\Delta)}{C(\Delta)} \ll \varepsilon^2.$$

With this estimate, for $|\Delta|$ sufficiently large, the height $h(x)$ can be bounded from below and from above by

$$c_1 \log|\Delta| - c_2 \leq h(x) \leq c\varepsilon^2 \log|\Delta| + 3\log\varepsilon^{-1} + c_4$$

and, by choosing ε properly, one gets a contradiction for $|\Delta|$ large enough. This implies that there are finitely many singular units.

3 No singular modulus is a unit

As we have seen in the previous paragraph, the proof of the finitness of singular units is not effective since it relies on an equidistribution result. Recently however, Yu. Bilu, P. Habegger and L. Kühne managed to prove in [2] the following

Theorem 3.1 *Singular units do not exist.*

Roughly speaking, this result is achieved by carrying out an effective version of the proof contained in [7] (and sketched above) and by improving the obtained bounds in order to be able to use computer assisted techniques.

The first step is to explicitely describe those $\tau \in \mathcal{H}$ such that $j(\tau)$ is a singular modulus of fixed discriminant Δ. For such a Δ define T_Δ as the set of triples of integers (a, b, c) such that

$$\begin{aligned} &\gcd(a, b, c) = 1, \qquad \Delta = b^2 - 4ac \\ &\text{either} \quad -a < b \leq a < c \quad \text{or} \quad 0 \leq b \leq a = c. \end{aligned}$$

A theorem of Gauss then asserts that

$$\{\tau_1, ..., \tau_m\} = \left\{ \frac{b + \sqrt{\Delta}}{2a} : (a, b, c) \in T_\Delta \right\}$$

is precisely the set of complex numbers τ in $\mathcal{H}$ such that $j(\tau)$ is a singular modulus of discriminant Δ. In this setting $m = C(\Delta)$ and the number $C_\varepsilon(\Delta)$ is precisely the number of triples $(a, b, c) \in T_\Delta$ such that $\tau = \tau(a, b, c)$ satisfies $\min\{|\tau - \zeta_6|, |\tau - \zeta_3|\} < \varepsilon\}$.

By using the explicit description above, the authors manage to prove that

$$C_\varepsilon(\Delta) \leq |\Delta|^{\frac{1}{2}+o(1)} \cdot \varepsilon + |\Delta|^{o(1)}. \tag{4}$$

Combining this estimate with the inequality (3) and optimizing ε, they deduce that the height of a singular modulus x of discriminant Δ is effectively bounded by

$$h(x) \ll \frac{|\Delta|^{o(1)}}{C(\Delta)} + \log \frac{|\Delta|^{\frac{1}{2}}}{C(\Delta)} + o(\log |\Delta|) \tag{5}$$

all the implicit constants being explicitely computable. This removes the ineffectivity of the upper bound that was present in Habegger's proof.

As far as the lower bounds for $h(x)$ are concerned, the authors prove the following two inequalities:

(HL) $h(x) \geq \frac{3}{\sqrt{5}} \log |\Delta| - 9.79.$

(EL) $h(x) \geq \frac{\pi |\Delta|^{\frac{1}{2}} - 0.01}{C(\Delta)}.$

The first estimate is an improvment of inequality (1), improvment needed due to numerical purposes. The second estimate follows essentially from the definition of Weil height and from the explicit description of singular moduli seen above.

By combining (5)+(HL) when $C(\Delta)$ is big, while using (5)+(EL) when $C(\Delta)$ is small, the authors conclude that, if a singular unit exists, its discriminant is bounded by

$$|\Delta| < 10^{15}.$$

However this bound is still too big to allow numerical computations. Hence the rest of the proof is dedicated to refining the bound above. First, the range $10^{10} \leq |\Delta| < 10^{15}$ is ruled out by sharpening estimate (4) on $C_\varepsilon(\Delta)$; the techniques used in this step are a combination of analytic number theory and numerical computations on SAGE. The range $|\Delta| < 10^{10}$ is then studied by further computer-assisted arguments. The conclusion is that singular units do not exist.

References

[1] Y. André, *Finitude des couples dâĂŹinvariants modulaires singuliers sur une courbe algébrique plane non modulaire*. J. Reine Angew. Math. **505** (1998), 203-208.

[2] Yu. Bilu, P. Habegger and L. Kühne, *No singular modulus is a unit*. To appear in Internat. Math. Res. Notices IMRN.

[3] Yu. Bilu, D. Masser and U. Zannier, *An effective "Theorem of André" for CM-points on a plane curve*. Math. Proc. Camb. Philos. Soc. **154** (2013), 145-152.

[4] L. Clozel and E. Ullmo, *Èquidistribution des points de Hecke*. Contribution to automorphic forms, geometry and number theory, Johns Hopkins Univ. Press **419** (2004), 193-254.

[5] P. Colmez, *Sur la hauteur de Faltings des variétés abéliennes à multiplication complexe*. Compositio Math. **111** (1998), 359-368.

[6] W. Duke, *Hyperbolic distribution problems and half-integral weight Maass forms*. Invent. Math. **92** (1988), 73-90.

[7] P. Habegger, *Singular moduli that are algebraic units*. Algebra and Number Theory **9** (2015), 1515-1524.

[8] L. Kühne, *An effective result of André-Oort type*. Ann. Math. **176** (2012), 651-671.

[9] Y. Nakkajima and Y. Taguchi, *A generalization of the Chowla-Selberg formula*. J. Reine Angew. Math. **419** (1991), 119-124.

Francesco Campagna
Department of Mathematical Sciences
University of Copenhagen
Universitetsparken 5
2100, Copenhagen, Denmark.
email: campagna@math.ku.dk

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 5, *Number* 1, *March* 2022, *pages* 17- 26

Peter Stevenhagen

Elliptic curves and primes of cyclic reduction

Written by Raiza Corpuz

1 Introduction

Let K be a number field. An *elliptic curve over* K is a nonsingular projective cubic curve with affine equation

$$E/K : Y^2 = X^3 + AX + B, \quad \text{where } A, B \in K.$$

The set of its K-rational points $E(K)$ has a natural group structure with the point 'at infinity' $(0 : 1 : 0)$ in $\mathbb{P}^2(K)$ taken as its zero element. In fact, the Mordell-Weil theorem asserts that $E(K)$ is a finitely generated abelian group, so we can write it as follows:

$$E(K) \cong E(K)_{\text{tor}} \oplus \mathbb{Z}^r.$$

The *torsion subgroup* $E(K)_{\text{tor}}$ consists of the points of finite order in $E(K)$ and the number r is the *free rank* of $E(K)$.

We go back to the affine equation of the elliptic curve. We take $A, B \in O_K$ integral and define the *discriminant* Δ_E of the elliptic curve E as 16 times the discriminant of the cubic polynomial on the right hand side of the equation. More explicitly,

$$\Delta_E = -16\left(4A^3 + 27B^2\right).$$

The discriminant is a value that helps determine whether an elliptic curve remains nonsingular or becomes singular after reducing the coefficients of its affine equation modulo a prime $\mathfrak{p} \subset O_K$. In particular, if $\mathfrak{p}$ is a prime that does not divide Δ_E, then we get a nonsingular reduction of E and we call $\mathfrak{p}$ a prime of *good reduction*. On the other hand, if $\mathfrak{p}$ divides Δ_E, then E reduces to a singular curve and we call $\mathfrak{p}$ a prime of *bad reduction*. The *j-invariant* of an elliptic curve is defined to be

$$j(E) = 1728 \cdot \frac{64A^3}{\Delta_E}.$$

Two elliptic curves over K are isomorphic over the algebraic closure $\overline{K}$ if and only if their j-invariants are the same. So the j-invariant partitions the collection of all elliptic curves over K into isomorphism classes over $\overline{K}$.

Consider a prime of good reduction $\mathfrak{p}$ in the ring of algebraic integers O_K of K, and let $k_\mathfrak{p} = O_K/\mathfrak{p}$ be the residue class field, which is finite of order $N_\mathfrak{p}$. The group of points of the reduction $E(k_\mathfrak{p})$ is a finite abelian group of order $N_\mathfrak{p} + 1 - a_\mathfrak{p}$, where $|a_\mathfrak{p}| \leq 2\sqrt{N_\mathfrak{p}}$. This bound for the order of $E(k_\mathfrak{p})$ follows from the Hasse-Weil theorem. Now the group $E(k_\mathfrak{p})$ has at most two generators, and so a natural question to ask is how many such reductions are cyclic. If the answer happens to be infinite, it is natural to ask whether these primes form some fraction of the full set of primes in O_K. This means computing, if it exists, the limit

$$\delta_{\text{cyc}} = \lim_{n\to\infty} \frac{a(n)}{\pi_K(n)},$$

where $a(n)$ is a function that counts the number of primes $\mathfrak{p} \in O_K$ with norm $N(\mathfrak{p}) \leq n$ for which $E(k_\mathfrak{p})$ is cyclic, and $\pi_K(n)$ simply counts all the primes in O_K with norm at most n. If it exists, δ_{cyc} is a number within $[0, 1]$. We refer to δ_{cyc} as the density of the set of primes of cyclic reduction.

Number theory is riddled with various density problems such as the one above. As an example, we take a look at Mersenne primes, which

are prime numbers of the form $2^p - 1$, where p is a prime. Although its infinitude is still in question, because they are close to powers of 2, there can only be at most $\log_2 n$ of them up to n. If there are infinitely many of them, then putting them up against the full set of primes gives us a density of 0. Generally, computing a density is nontrivial. To compute for a density, one often imposes splitting conditions in finite Galois extensions for the primes one wishes to count, then use analytic number theory compute an asymptotic limit.

2 Known results

Let $\mathfrak{p}$ be a prime of good reduction. The injectivity of the reduction modulo $\mathfrak{p}$ map (cf. [9] Chapter VII.3 Proposition 3.1) tells us that if $E(K)_{\text{tor}}$ is non-cyclic, that is, $\#E(K)[\ell] = \ell^2$ for some prime ℓ, then $E(k_\mathfrak{p})$ is almost always non-cyclic. It is a fact that when $\#E(K)[\ell] = \ell^2$, then $E(\overline{K})[\ell] \subseteq E(K)$, and this implies that the primitive ℓ^{th}-root of unity $\zeta_\ell = e^{\frac{2\pi i}{\ell}}$ is contained in K. For $K = \mathbb{Q}$, this only happens for $\ell = 2$. In this case, the necessary condition that $E/\mathbb{Q}$ does not have full 2-torsion is actually sufficient.

Theorem 1 *(Gupta-Murty, 1990, [4]) Let $E/\mathbb{Q}$ be an elliptic curve. $E(\mathbb{Q})$ does not have full 2-torsion if and only if $E(\mathbb{F}_p)$ is cyclic for infinitely many prime numbers p.*

Over general number fields K, it is possible that $E(K)_{\text{tor}}$ is cyclic, or even trivial, but $E(k_\mathfrak{p})$ is non-cyclic for almost all $\mathfrak{p}$ ([1], Theorem 4.1). Moreover, the proof of Theorem 1 does not tell us anything about the density of the primes p for which $E(\mathbb{F}_p)$ is cyclic. And so instead of generalizing Theorem 1 over arbitrary number fields, we proceed by finding a way to describe the cyclicity of $E(k_\mathfrak{p})$ in terms of the splitting behavior of $\mathfrak{p}$ in extensions of K, following Serre.

We denote by $K_\ell = K(E(\overline{K})[\ell])$ the ℓ-division field of $E(K)$. One can view K_ℓ as the smallest Galois extension of K over which the points in $E(\overline{K})[\ell]$ are defined.

Lemma 1 *Suppose* $\mathfrak{p}$ *is a prime ideal not dividing* $\Delta_E \cdot \Delta_K$. *Then* $E(k_\mathfrak{p})$ *is cyclic if and only if* $\mathfrak{p}$ *does not split completely in* K_ℓ *for any prime number* ℓ.

This lemma resembles Artin's primitive root conjecture: let a be an integer different from -1 and let p be a prime not dividing $2a$. Then a is a primitive root modulo p, that is $\mathbb{F}_p^* = \langle a \bmod p \rangle$, if and only if p does not split completely in any field $F_\ell = \mathbb{Q}\left(\zeta_\ell, \sqrt[\ell]{a}\right)$. Here, F_ℓ is the splitting field of $X^\ell - a$ over $\mathbb{Q}$. Originally, Artin conjectured that the density of primes p for which a is a primitive root modulo p is

$$\delta_a = \prod_{\substack{\ell \geq 2 \\ \text{prime}}} \left(1 - \frac{1}{[F_\ell : \mathbb{Q}]}\right). \tag{1}$$

The idea of Artin was to fix a prime ℓ and compute the density of primes that do not split completely in F_ℓ. This is precisely the value $1 - \frac{1}{[F_\ell:\mathbb{Q}]}$. Assuming that the fields F_ℓ are linearly disjoint over $\mathbb{Q}$, as in the case for Artin's original example when $a = 2$, then we can compute the density of the primes p for which a is a primitive root modulo p by taking the product of $1 - \frac{1}{[F_\ell:\mathbb{Q}]}$ over all primes ℓ. This results to the *naive density* δ_a in (1). The problem is that the fields F_ℓ are in general not linearly disjoint. For instance, when $a = 5$, then we have $F_2 = \mathbb{Q}(\sqrt{5})$ and $F_5 = \mathbb{Q}(\zeta_5, \sqrt[5]{5})$, hence $F_2 \subset F_5$. So if $\mathfrak{p}$ does not split in F_2 then it does not split in F_5 either.

Now one can take the dependencies between the fields F_ℓ into account by correctly computing the degrees $[F_n : \mathbb{Q}]$ of their composita F_n, and then obtaining the right conjectural density after an inclusion-exclusion argument. This corrected statement was proved by Hooley under the assumption of the generalized Riemann hypothesis.

Theorem 2 *(Hooley, 1967, [5]) Let* $a \in \mathbb{Z} \setminus \{-1\}$ *that is not a square. Assuming the generalized Riemann hypothesis,* $\mathbb{F}_p^* = \langle a \bmod p \rangle$ *for a*

set of primes p of density

$$\delta_a = \sum_{n=1}^{\infty} \frac{\mu(n)}{[F_n : \mathbb{Q}]},$$

where μ is the Möbius function.

Around a decade later, Serre proved an analog of Hooley's theorem for elliptic curves.

Theorem 3 *(Serre, 1978, [8]) Let $E/\mathbb{Q}$ be an elliptic curve. Assuming the generalized Riemann hypothesis, $E(\mathbb{F}_p)$ is cyclic for a set of primes p of density*

$$\delta_{cyc} = \sum_{n=1}^{\infty} \frac{\mu(n)}{[K_n : \mathbb{Q}]}.$$

Here, $K_n = \mathbb{Q}(E(\overline{\mathbb{Q}})[n])$.

Campagna and Stevenhagen generalized this above theorem by Serre to elliptic curves over arbitrary number fields [1]. In practice however, this is still not entirely satisfying because the convergence of the sum for δ_{cyc} is slow, and it is not clear when it is positive. Lenstra observed that in the case of primitive root problems, the vanishing of densities is always caused by incompatibility of conditions involving finitely many fields F_ℓ [6].

3 Main results

Guided by Lenstra's idea, Campagna and Stevenhagen singled out the fields K_ℓ that prove to be problematic to the elliptic density. These are the fields K_ℓ that can give rise to 'entanglement', meaning we get non-linearly disjoint extensions K_ℓ/K. To treat these entanglements, Theorem 3 is applied, otherwise, the naive density is computed.

Overall, there are two distinct cases depending on whether or not an elliptic curve E/K has complex multiplication. Due to the existence of the multiplication-by-n map, it is easy to see that $\mathbb{Z}$ may be embedded into the endomorphism ring $\mathrm{End}(E)$ of E. For fields of characteristic 0, if $\mathrm{End}(E)$ is strictly larger than $\mathbb{Z}$, then $\mathrm{End}(E)$ is isomorphic to an order $R \subset F$, where F is an imaginary quadratic field. In this case we say that E has *complex multiplication* by R.

Theorem 4 *(Campagna and Stevenhagen, 2018, [1]) Let E/K be an elliptic curve without complex multiplication. Then there exists an integer $N = N(E,K) \in \mathbb{Z}_{>0}$ such that δ_{cyc} can be factored as*

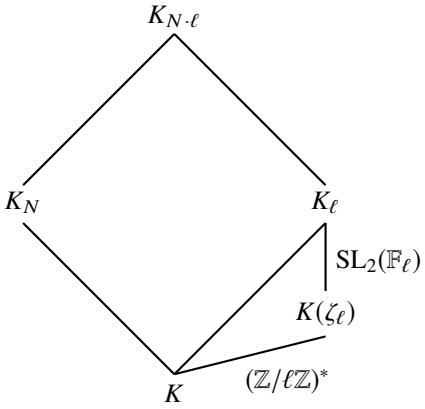
$$\delta_{cyc} = \sum_{m|N} \frac{\mu(m)}{[K_m : K]} \prod_{\substack{\ell \nmid N \\ \text{prime}}} \left(1 - \frac{1}{[K_\ell : K]}\right).$$

We can take for $N(E,K)$ any positive integer divisible by the product of: the small primes 2, 3 and 5, the primes dividing the discriminant Δ_K of K, the primes dividing the norms of the primes of bad reduction of E, and the primes ℓ for which the degree of K_ℓ is not maximal.

By Serre's open image theorem [7], we know that for an elliptic curve E/K without complex multiplication over the algebraic closure $\overline{K}$, for almost all $\ell \in \mathbb{N}$, the map

$$\rho_\ell : \mathrm{Gal}(K_\ell/K) \to \mathrm{GL}_2(\mathbb{F}_\ell)$$

is an isomorphism and K_ℓ has maximal degree $\#\,\mathrm{GL}_2(\mathbb{F}_\ell) = (\ell^2-1)(\ell^2-\ell)$ over K. Group theoretical results and the Jördan-Holder theorem show that for N as in the Theorem, the fields K_ℓ and K_N are linearly disjoint over K, making splitting in K_ℓ independent of splitting in K_N. This enables us to compute the density corresponding to the finitely many fields K_ℓ where entanglements happen separately.



The case when E is an elliptic curve with complex multiplication is different because the fields K_ℓ, as we remarked earlier, may not be linearly disjoint. To illustrate this case, consider the elliptic curve

$$E/\mathbb{Q} : Y^2 = X^3 - 35X - 98 = (X-7)(X^2+7X^2+14).$$

Since $K_2 = \mathbb{Q}(\sqrt{-7})$ is the splitting field of $X^3 - 35X - 98$ over $\mathbb{Q}$, E does not have full 2-torsion.

There are 13 isomorphism classes of rational elliptic curves with complex multiplication and their j-invariants correspond to the list of orders of class number 1. So knowing that $j(E) = -3375$ tells us that our E has complex multiplication by $\mathcal{O}_{K_2} = \mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right]$. In other words, K_2 coincides with the CM-field $F = \mathbb{Q}(\sqrt{-7})$ of E. And since for any prime $\ell \geq 3$, we have $F \subset K_\ell$, then the field K_2 is always contained in the field K_ℓ. As a consequence, if p does not split completely in K_2, then it also does not split completely in K_ℓ for any odd prime ℓ.

From here we use Lemma 1 which says that the splitting of p in $\mathbb{Q}(\sqrt{-7})$ is a necessary and sufficient condition for the non-cyclicity of $E(\mathbb{F}_p)$. This happens precisely when $p \equiv 1, 2, 4 \pmod 7$, and so we have

$$E(\mathbb{F}_p) \text{ is cyclic} \iff p \equiv 3, 5, 6 \pmod 7.$$

In this particular example, we can deduce that $\delta_{\text{cyc}} = \frac{1}{2}$. In this case, splitting in K_2 is all we need to look at, so assuming that the generalized Riemann hypothesis is true is not necessary.

When E/K has complex multiplication by some order $\mathcal{O}$ in an imaginary field F, the density is computed in two different ways depending on whether or not K contains the CM field F. We define

$$A_{\mathcal{O},\ell} = 1 - \frac{1}{\#(\mathcal{O}/\ell\mathcal{O})^\times} = \begin{cases} 1 - (\ell - 1)^{-2} & \text{if } \left(\frac{D}{\ell}\right) = 1, \\ 1 - (\ell^2 - 1)^{-1} & \text{if } \left(\frac{D}{\ell}\right) = -1, \\ 1 - (\ell^2 - \ell)^{-1} & \text{if } \left(\frac{D}{\ell}\right) = 0, \end{cases}$$

and call

$$A_{\mathcal{O}} = \prod_{\ell \text{ prime}} A_{\mathcal{O},\ell}$$

the *Artin constant of the order* $\mathcal{O}$. Using the Chebotarev Density theorem, Campagna and Stevenhagen were able to formulate the following results.

Theorem 5 *(Campagna and Stevenhagen, [3]) Let E/K be an elliptic curve with complex multiplication by an order $\mathcal{O} \subset K$. Then the set of primes of cyclic reduction of E has density*

$$\delta_{cyc} = \sum_{m | T_{E/K}} \frac{\mu(m)}{[K_m : K]} \cdot \prod_{\ell \nmid T_{E/K}} A_{\mathcal{O},\ell}.$$

This case is reminiscent of Theorem 4, with $T_{E/K}$ being the integer product of the conductor $\mathfrak{f}_{\mathcal{O}} := [\mathcal{O}_F : \mathcal{O}] \in \mathbb{N}$ of the order $\mathcal{O}$, the absolute discriminant $\Delta_K \in \mathbb{Z}$ of the number field K, and the absolute norm $N_{K/\mathbb{Q}} := |\mathcal{O}_K/\mathfrak{f}_E| \in \mathbb{N}$ of the conductor ideal $\mathfrak{f}_E \subseteq \mathcal{O}_K$ of E.

When the field of definition K does not contain the CM field F, it is no longer true that the family of division fields $\{K_\ell\}_\ell$ for prime ℓ becomes linearly disjoint after removing a finite set of fields. The previous example is an illustration of this case. There we saw an instance wherein the CM field F is contained in K_ℓ for all primes $\ell \geq 3$.

Theorem 6 *(Campagna and Stevenhagen, [3]) Let E/K be an elliptic curve with complex multiplication by an order $\mathcal{O}$ with discriminant $\Delta_{\mathcal{O}} < -4$ in an imaginary quadratic field F and defined over $K \not\supseteq F$. Write $H_{2,\mathcal{O}}$ for the ray class field modulo 2 relative to the order $\mathcal{O}$. Then there exists a non-negative rational number $c_{E/K} \in \mathbb{Q}_{\geq 0}$ such that:*

1. *If $\Delta_{\mathcal{O}} \equiv 0 \pmod 4$, then either K is linearly disjoint from $H_{2,\mathcal{O}}$ over $\mathbb{Q}(j(E))$ and*

$$\delta_{cyc} = \frac{1}{4} + \frac{c_{E/K}}{2} \cdot A_{\mathcal{O}}$$

   or $K \cap H_{2,\mathcal{O}} \supsetneq \mathbb{Q}(j(E))$ and we have

$$\delta_{cyc} = \begin{cases} 0 & \text{if } K = K_2, \\ \frac{1}{2} & \text{otherwise.} \end{cases}$$

2. *If $\Delta_{\mathcal{O}} \equiv 5 \pmod 8$, then*

$$\delta_{cyc} = \frac{1}{2} + \frac{c_{E/K}}{2} \cdot A_{\mathcal{O}}.$$

3. *If $\Delta_{\mathcal{O}} \equiv 1 \pmod 8$, then $\delta_{cyc} = 1/2$.*

References

[1] F. Campagna and P. Stevenhagen, *Cyclic reduction of elliptic curves*. ArXiv:2001.00028v1.

[2] F. Campagna and P. Stevenhagen, *Cyclic reduction of CM elliptic curves*. In preparation.

[3] F. Campagna *Arithmetic and diophantine properties of elliptic curves with complex multiplication*. Thesis (2021).

[4] R. Gupta and R. Murty, *Cyclicity and generation of points mod p on elliptic curves*. Invent. Math. **101** (1990), 225-235.

[5] C. Hooley, *On Artin's conjecture*. J. Reine Angew. Math. **225** (1967), 209-220.

[6] H.W. Lenstra Jr., *On Artin's conjecture and Euclid's algorithm in global fields*. Invent. Math. **42** (1977), 201-224.

[7] J.P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*. Invent. Math. **15** (1972), 259-331.

[8] J.P. Serre, *Résumé des cours de 1977-1978*. Annuaire du Collége de France (1978), 67-70.

[9] J.H. Silverman, *The arithmetic of elliptic curves*, 2nd edition. Springer-Verlag Graduate Texts in Mathematics 106, 2009.

Raiza Corpuz
Institute of Mathematics
University of the Philippines Diliman
Diliman, Quezon City
1101 Philippines.
email: rcorpuz@math.upd.edu.ph

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 5, *Number* 1, *March* 2022, *pages* 27-31

Shabnam Akhtari

Lower bounds for the Mahler measures of polynomials that are sum of a bounded number of monomials

Written by Mahadi Ddamulira

The speaker presents a joint work with Jeffrey Vaaler [1], in which they extend a recent result of Dobrowolski and Smyth to establish a sharp lower bound for the Mahler measures of polynomials in any number of variables.

For a polynomial $f(z) \in \mathbb{C}[z]$ that is not identically zero, the logarithmic Mahler measure is defined as

$$m(f) = \int_0^1 \log \left| f(e^{2\pi i t}) \right| \mathrm{d}t.$$

The classical Mahler measure is then defined as

$$M(f) = \exp(m(f)).$$

Let

$$f(z) = c_N z^N + \cdots + c_1 z + c_0 = c_N (z - \alpha_1) \cdots (z - \alpha_N). \qquad (1)$$

Jensen's formula implies that

$$M(f) = \exp(m(f)) = |c_N| \prod_{n=1}^{N} \max\{1, |\alpha_n|\}. \tag{2}$$

From (2), it immediately follows that if $f(z)$ and $g(z)$ are nonzero polynomials in $\mathbb{C}[z]$, then

$$M(fg) = M(f)M(g).$$

The following result is a well-known lower bound due to Mahler.

Theorem 1 *Let $f(z)$ be a polynomial of degree N in $\mathbb{C}[z]$ given by* (1). *Then*

$$|c_n| \le M(f)\binom{N}{n} \quad \textit{for each} \quad n = 0, 1, 2, \ldots, N.$$

Note that, if $f(z) = (z \pm 1)^k$, then $M(f) = 1$, so in this example we have equality above.

The following result is due to Dobrowolski and Smyth (2016). Here, the height $H(f)$ of a polynomial f is the maximum modulus of its coefficients.

Theorem 2 *We have*

$$M(f) \ge \frac{H(f)}{2^{k-1}},$$

where $f(z) = a_0 z^{n_0} + \cdots + a_{k-1} z^{n_{k-1}} + a_k \in \mathbb{C}[z]$ and $n_0 > n_1 > \cdots > n_{k-1} > 0$.

Assume that $f(z)$ is a polynomial in $\mathbb{C}[z]$ that is not identically zero, and assume that $f(z)$ is given by

$$f(z) = c_0 z^{n_0} + c_1 z^{n_1} + \cdots + c_N z^{n_N}, \tag{3}$$

where N is a non-negative integer and $n_0, n_1, \ldots, n_N$ are non-negative integers such that

$$n_0 < n_1 < \cdots < n_N.$$

The speaker presents the main result in which they establish a lower bound for $M(f)$ which depends on the coefficients and on the number of monomials, but does not depend on the degree of f.

Theorem 3 (S. Akhtari, J. Vaaler (2018)) *Let $f(z)$ be a polynomial in $\mathbb{C}[z]$ that is not identically zero, and is defined by* (3)*. Then we have*

$$M(f) \geq \frac{|c_n|}{\binom{N}{n}}, \quad \textit{for all } n,\ 0 \leq n \leq N-1.$$

A consequence of these results

Let $f : \mathbb{R}/\mathbb{Z} \to \mathbb{C}$ be a trigonometric polynomial, not identically zero, and a sum of at most $N+1$ distict characters. Then, we can write f as

$$f(t) = \sum_{n=0}^{N} c_n e(m_n t), \tag{4}$$

where $c_0, c_1, \ldots, c_N$ are complex coefficients, and $m_0, m_1, \ldots, m_N$ are integers such that

$$m_0 < m_1 < \cdots < m_N.$$

Since f is not identically zero, the Mahler measure of f is a positive number given by

$$M(f) = \exp\left(\int_{\mathbb{R}/\mathbb{Z}} \log|f(t)| \mathrm{d}t\right).$$

Corollary 4 *Let $f(t)$ be a trigonometric polynomial with complex coefficients that is not identically zero, and given by* (4)*. Then we have*

$$|c_n| \leq M(f)\binom{N}{n} \quad \textit{for each} \quad n = 0, 1, 2, \ldots, N.$$

For positive integers M, the speaker states an extension of Corollary 4 to trigonometric polynomials

$$F : (\mathbb{R}/\mathbb{Z})^M \to \mathbb{C}$$

that are not identically zero. The Fourier transform of F is the function

$$\hat{F} : \mathbb{Z}^M \to \mathbb{C},$$

defined at each lattice point $\mathbf{k}$ in $\mathbb{Z}^M$ by

$$\hat{F}(\mathbf{k}) = \int_{(\mathbb{R}/\mathbb{Z})^M} F(\mathbf{x}) e(-\mathbf{k}^T \mathbf{x}) \mathrm{d}\mathbf{x}.$$

Since F is not identically zero, the Mahler measure of F is a positive number given by

$$M(F) = \exp\left(\int_{(\mathbb{R}/\mathbb{Z})^M} \log |F(\mathbf{x})| \mathrm{d}\mathbf{x} \right).$$

Assume that $\mathfrak{S} \subseteq \mathbb{Z}^M$ is non-empty finite set that contains the support of $\mathbf{F}$. That is, assume that

$$\{\mathbf{k} \in \mathbb{Z}^M : \hat{F}(\mathbf{k}) \neq 0\} \subseteq \mathfrak{S},$$

and thus, F has the representation

$$F(\mathbf{x}) = \sum_{\mathbf{k} \in \mathfrak{S}} \hat{F}(\mathbf{k}) e(\mathbf{k}^T \mathbf{x}). \tag{5}$$

If $\alpha = (\alpha_m)$ is a (column) vector in $\mathbb{R}^M$, we write

$$\varphi_\alpha : \mathbb{Z}^M \to \mathbb{R}$$

for the homomorphism given by

$$\varphi_\alpha(\mathbf{k}) = \mathbf{k}^T \alpha = k_1 \alpha_1 + \cdots + k_M \alpha_M .$$

It is easy to verify that φ_α is an injective homomorphism if and only if the coordinates $\alpha_1, \ldots, \alpha_M$ are $\mathbb{Q}$-linearly independent real numbers. Let the nonempty, finite set $\mathfrak{S} \subseteq \mathbb{Z}^M$ have cardinality $N+1$, where $0 \leq N$. If φ_α is an injective homomorphism, then the set

$$\{\varphi_\alpha(\mathbf{k}) : \mathbf{k} \in \mathfrak{S}\}$$

consists of exactly $N+1$ real numbers. It follows that the set $\mathfrak{S}$ can be indexed so that

$$\mathfrak{S} = \{\mathbf{k}_0, \mathbf{k}_1, \ldots, \mathbf{k}_N\}, \tag{6}$$

and

$$\varphi_\alpha(\mathbf{k}_0) < \varphi_\alpha(\mathbf{k}_1) < \cdots < \varphi_\alpha(\mathbf{k}_N) \tag{7}$$

The following result is a generalization of Corollary 4.

Theorem 5 *Let $F : (\mathbb{R}/\mathbb{Z})^M \to \mathbb{C}$ be a trigonometric polynomial that is not identically zero, and is given by* (5)*. Let $\varphi_\alpha : \mathbb{Z}^M \to \mathbb{R}$ be an injective homomorphism, and assume that the finite set $\mathfrak{S}$, which contains the support of $\hat{F}$, is indexed so that* (6) *and* (7) *hold. Then we have*

$$\left|\hat{F}(\mathbf{k}_n)\right| \leq M(F)\binom{N}{n} \quad \textit{for each} \quad n = 0, 1, 2, \ldots, N.$$

References

[1] S. Akhtari and J. D. Vaaler, *Lower bounds for the Mahler measures of polynomials that are sum of a bounded number of monomials.* Int. J. Number Theory **15** (7) (2019), 1425-1436.

Mahadi Ddamulira
Institute of Analysis and Number Theory
Graz University of Technology
Kopernikusgasse 24/II
8010 Graz, Austria.
email: mddamulira@tugraz.at; mahadi@aims.edu.gh

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 5, *Number* 1, *March* 2020, *pages* 33-39

Andrew Granville

Multiplicative functions in short intervals and arithmetic progressions

Written by Alessandro Fazzari

1 The multiplication table

For any integer $N > 1$, one can consider the multiplication table, which has N^2 entries. Because of the symmetry relative to the diagonal, the number of different entries $M(N)$ is actually smaller than N^2. In addition an integer might have several representations as a product of two integers, for example $6 \cdot 2 = 12 = 3 \cdot 4$ appears four times in the multiplication table up to 10. Hence $M(N)$ is even smaller, for instance $M(10) = 42$. The natural question one may ask is how large $M(N)$ is with respect to N^2.
In 1955 Erdős proved that

$$\frac{M(N)}{N^2} \to 0 \tag{1}$$

as $N \to \infty$ and the basic idea in order to show this result can be described as follows. Denoting with $\Omega(n)$ the function that counts the total number of prime factors of an integer n, we recall that $\Omega(n) \sim$

$\log\log n$ for almost every n. Then an integer in the set $\{ab : a, b \leq N\}$ has typically $\log\log N + \log\log N = 2\log\log N$ prime factors. On the other hand, a typical integer in $\{n : n \leq N^2\}$ has $\log\log N^2 = \log\log N + \log 2$ prime factors. This means that, up to few exceptions, the typical integer in the latter set does not belong to the former. Since $M(N)$ and N^2 are the cardinality of these two sets respectively, (1) follows.

In order to investigate the correct order of $M(N)$, given an integer $\frac{N^2}{2} \leq n < N^2$, one has to count the number of representations of n as a product ab, with $a, b \leq N$. Notice that since $n = ab$ one has $\frac{N}{2} < a, b \leq N$. Thus one is lead to the question of counting the divisors of n in intervals of multiplicative length 2, i.e.

$$\sharp\{n : \exists d | n\,,\ Y < d < 2Y\}.$$

Showing that a typical integer does not have a divisor in a given dyadic interval, in [1] Ford proved that

$$M(N) \asymp \frac{N^2}{(\log N)^c (\log\log N)^{3/2}} \quad \text{where} \quad c := 1 - \frac{1 + \log\log 2}{\log 2}.$$

The results of this article also give that for almost all primes p such that $\frac{x}{2} < p < x$, one has that $p - 1$ does not have a divisor in a given dyadic interval $(Y, 2Y)$, as Y goes to infinity with N.

2 Multiplicative functions in arithmetic progressions

A classical problem in analytic number theory is that of estimating the number $\pi(x; a, q)$ of primes up to x, which are congruent to $a \pmod q$ for some a, q with $(a, q) = 1$. If q is small, this is asymptotic to the total number of primes up to x divided by the number of integers coprime to q. In general one expects

$$\pi(x; a, q) - \frac{\pi(x)}{\phi(q)} \tag{2}$$

to be small. As usual π denotes the counting function of primes and ϕ the Euler totient function. This is really difficult to prove unless x is large with respect to q but the Bombieri-Vinogradov theorem shows that this is true on average, even if we pick the worst case for any modulus and then we sum over q up to Q. Specifically, for any fixed $A > 0$ there exists $B = B(A) > 0$ such that if $Q \leq x^{1/2}(\log x)^{-B}$ we have

$$\sum_{q \leq Q} \max_{(a,q)=1} \left| \pi(x; a, q) - \frac{\pi(x)}{\phi(q)} \right| \ll \frac{x}{(\log x)^A}. \tag{3}$$

Roughly speaking, this theorem does not prove that (2) is small for every arithmetic progression, but it shows that this is true on average. Hence even if the approximation fails, it does not happen often.
This kind of analysis is still of great interest when we replace π with any multiplicative function f such that $|f(n)| \leq 1$. In this case one wants to study

$$\sum_{\substack{n \leq x \\ n \equiv a \ (q)}} f(n) - \frac{1}{\phi(q)} \sum_{\substack{n \leq x \\ (n,q)=1}} f(n) \tag{4}$$

but unfortunately this is not always small. As we are going to see, there are two obstructions towards the Bombieri-Vinogradov theorem for f

$$\sum_{q \leq \sqrt{x}(\log x)^{-B}} \max_{(a,q)=1} \left| \sum_{\substack{n \leq x \\ n \equiv a \ (q)}} f(n) - \frac{1}{\phi(q)} \sum_{\substack{n \leq x \\ (n,q)=1}} f(n) \right| \ll \frac{x}{(\log x)^A} \tag{5}$$

which measures how well f is well-distributed "on average" in arithmetic progressions with moduli $q \leq \sqrt{x}(\log x)^{-B}$.

Let's analyze the first problem. If one picks $f(n) = (\frac{n}{3})$ the quadratic character (mod 3), then f is not well-distributed in arithmetic progressions (mod q) if $3|q$. Of course (4) is not small, since for instance in the case $a = 1$ the first term is $\frac{x}{q}$ while the second essentially vanishes. In order to prove a Bombieri-Vinogradov type theorem, we need to avoid this problem which appears when f is strongly correlated with

a character of small conductor. By analogy with the classical proof of the Bombieri-Vinogradov theorem, one can sort this problem out by assuming a Siegel-Walfisz type theorem, i.e. if $(a, q) = 1$ then

$$\sum_{\substack{n\leq x\\ n\equiv a\ (q)}} f(n) - \frac{1}{\phi(q)} \sum_{\substack{n\leq x\\ (n,q)=1}} f(n) \ll_A \frac{x}{(\log x)^A} \tag{6}$$

which removes the influence of the bad characters with small moduli. Actually even if (6) does not hold, one can prove a Bombieri-Vinogradov type theorem, by understanding the structure of the problem given by the bad moduli (see [3]).

There is also a second problem if we are looking for a good estimate for (4). Let f be a multiplicative function such that $f(p) = 1$ for all $\frac{x}{2} < p < x$ such that $p - 1$ has no divisors between Q and $2Q$ and $f(p) = 0$ for all the other primes up to x. As we said before, in view of [1], it is known that $p - 1$ has typically no divisors in a dyadic interval. For such an f one has

$$\sum_{\substack{n\leq x\\ n\equiv 1\ (q)}} f(n) - \frac{1}{\phi(q)} \sum_{\substack{n\leq x\\ (n,q)=1}} f(n) \gg \frac{x}{\phi(q)\log x}$$

for any $q \in (Q, 2Q)$ and this gives an obstruction to a Bombieri-Vinogradov theorem since it implies

$$\sum_{Q<q<2Q} \Big| \sum_{\substack{n\leq x\\ n\equiv 1\ (q)}} f(n) - \frac{1}{\phi(q)} \sum_{\substack{n\leq x\\ (n,q)=1}} f(n)\Big| \gg \frac{x}{\log x}.$$

This problem comes out when the values of $f(p)$ conspire against the equidistribution, misbehaving on many large primes p. In order to get rid of this obstruction, one can just consider multiplicative functions f which are supported on small primes, say $p \leq x^{1/2}$. In this way one is in the situation where this second problem does not exist and a

Bombieri-Vinogradov type theorem can be proved. This can be found in [4], where the authors are also able to go beyond the $x^{1/2}$-barrier if f is smooth-supported.

Actually one can avoid the obstruction of large primes even without any assumption of the function's support, trying to understand for which f the Bombieri-Vinogradov theorem (5) holds. Of course a Siegel-Walfisz assumption like (6) is not enough, what else do we need? A big part of the argument in the proof of the classical Bombieri-Vinogradov theorem relates the distribution of 1_P to the distribution of μ, bringing into play the convolution inverse of 1. In view of this, let f be a 1-bounded multiplicative function (see [5] for further details) and g its convolution inverse. Evidently if (5) holds for both f and g then (6) holds for f and g. Can one get the other implication? One sees that the other implication turns out to be true if (5) also holds for $f \cdot 1_P$. In other words, the Bombieri-Vinogradov theorem holds for both f and g if and only if the Bombieri-Vinogradov theorem holds for $f \cdot 1_P$ and Siegel-Walfisz holds for both f and g.

3 Multiplicative functions in short intervals

Recently Matomäki and Radziwiłł made important progress on the understanding of multiplicative functions in short intervals. In [6], given a multiplicative function $f : \mathbb{N} \to [-1, 1]$, they study f in short intervals of length y. They compare the mean value between x and $x + y$

$$\frac{1}{y} \sum_{x \leq n \leq x+y} f(n)$$

with the average over the whole interval $[1, x]$:

$$\frac{1}{x} \sum_{n \leq x} f(n).$$

They proved that the difference is almost always small, provided that y goes to infinity with x. Now the aim is to prove it for every x, removing the "almost" from the statement. Huxley proved something in this direction, for $y = x^{7/12+\epsilon}$ and f the indicator function of primes. Moreover in [2] Granville, Harper and Soundararajan consider this problem for multiplicative functions and $y = x^{1-\delta}$, with $\delta \to 0^+$ and all x. Granville and Harper are still working with Matomäki and Radziwiłł with the hope that a combination of their techniques would improve this result. They essentially have reached $x^{7/12+\epsilon}$ in general and they are looking at further hypotheses that would allow to go down to as small as $x^{1/2+\epsilon}$.

References

[1] K. Ford, *The distribution of integers with a divisor in a given interval*. In: Ann. of Math., 168 (2008), 367âĂŞ433.

[2] A. Granville, A. Harper and K. Soundararajan, *A new proof of Halasz's Theorem, and its consequences*. In: Compositio Mathematica 155 (2019), 126-163.

[3] A. Granville and X. Shao, *Bombieri-Vinogradov for multiplicative functions, and beyond the $x^{1/2}$-barrier*. In: arXiv:1703.06865v1 [math.NT].

[4] A. Granville, S. Drappeau and X. Shao, *Smooth-supported multiplicative functions in arithmetic progressions beyond the $x^{1/2}$-barrier*. In: arXiv:1704.04831v2 [math.NT].

[5] A. Granville and X. Shao, *When does the Bombieri-Vinogradov Theorem hold for a given multiplicative function?*. In: arXiv:1706.05710v1 [math.NT].

[6] K. Matomäki, M. Radziwiłł, *Multiplicative functions in short intervals*. In: arXiv:1502.02374 [math.NT]

Alessandro Fazzari
Dipartimento di Matematica
Università di Genova
Via Dodecaneso 35
16146, Genova, Italia.
email: fazzari@dima.unige.it

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 5, *Number* 1, *March* 2020, *pages* 41-49

David Kohel

Orienting Supersingular Isogeny Graphs

Written by Boris Fouotsa Tako

1 Introduction

Given an elliptic curve E over a field k, and a finite set of primes S, we can associate an *isogeny graph* $\Gamma = \Gamma(E, S)$:

- whose vertices are isomorphism classes (j-invariants) of elliptic curves $\overline{k}$-isogenous to E, and
- whose edges are isogenies of degree $l \in S$.

If $S = \{l\}$, then we call Γ an l-isogeny graph. The l-isogeny graph of E is $(l + 1)$-regular.

In characteristic 0, if $End(E) = \mathbb{Z}$, this graph is a tree; if E has complex multiplication by an order $\mathcal{O}$ in an imaginary quadratic field K ($\mathbb{Z} \subsetneq End(E) = \mathcal{O} \subset \mathcal{O}_K$) and l is a split prime in K, then there is a cycle in $\Gamma(E, \{l\})$.

Over a finite field of characteristic p, the isogeny graph can be distinguish as ordinary (which is a faitfull image of a CM isogeny graph), or supersingular. The idea of *orienting* a supersingular graph is to lift the supersingular graph back to a CM isogeny graph.

The supersingular isogeny graphs are remarkable because the vertex sets are finite: $[\frac{p}{12}]+\epsilon_p$ curves. Moreover, taking a representative curve $E/\mathbb{F}_p$, with $|E(\mathbb{F}_p)| = p + 1$, all l-isogenies are defined over $\mathbb{F}_{p^2}$.

Supersingular isogeny graphs have been proposed for

- cryptographic hash functions [2],
- the post-quantum SIDH (Supersingular Isogeny Diffie-Hellman) key exchange protocol [5].

A new key exchange protocol, CSIDH (Commutative SIDH) [1], analogous to SIDH, uses only $\mathbb{F}_p$-rational elliptic curves and $\mathbb{F}_p$-rational isogenies. The constraint to $\mathbb{F}_p$-rational isogenies can be interpreted as an *orientation* of the supersingular graph by the subring $\mathbb{Z}[\pi]$ of $End(E)$.

We introduce a category of $\mathcal{O}$-oriented supersingular elliptic curves and derive the properties of the associated oriented and nonoriented supersingular l-isogeny graphs. As application, we introduce an Oriented Supersingular Isogeny Diffie-Hellman (OSIDH) protocol generalizing the CSIDH protocol.

2 Orientations and class group action

Let $\mathcal{O}$ be an order in an imaginary quadratic field K. An *$\mathcal{O}$-orientation* of a supersingular elliptic curve E is an inclusion $\iota : \mathcal{O} \to End(E)$, and a *$K$-orientation* of a supersingular elliptic curve E is an inclusion $\iota : K \to End(E) \otimes_{\mathbb{Z}} \mathbb{Q}$. An $\mathcal{O}$-orientation is said to be *primitive* if $\mathcal{O} \cong \iota(K) \cap End(E)$.

Theorem 2.1 *The category of K-oriented supersingular elliptic curves (E, ι), whose morphisms are isogenies commuting with the K-orientations, is equivalent to the category of elliptic curves with CM by K.*

One feature of the l-isogeny graph of CM elliptic curves is that in each component, depending on wether l is split, inert or ramified in K, there is a cycle of vertices, unique vertex or adjacent pair of vertices which have l-maximal endomorphism ring.

Chains of l-isogenies leading away from these l-maximal vertices have successively (and strictly) smaller endomorphim rings, by a power of l. They are called *descending l-isogeny chains*.

This let us define the *depth* of a CM elliptic curve in the l-isogeny graph as the valuation of the index $[\mathcal{O}_K : End(E)]$ at l, which measures the smallest distance to an l-maximal vertex. Consequently, we obtain a notion of depth at l in the K-oriented supersingular l-isogeny graph.

The set $SSO(\mathbb{F}_{p^2}, \mathcal{O})$ of primitive $\mathcal{O}$-oriented supersingular elliptic curves is equiped with an action of the class group $Cl(\mathcal{O})$:

$$\begin{array}{rcl} Cl(\mathcal{O}) \times SSO(\mathbb{F}_{p^2}, \mathcal{O}) & \to & SSO(\mathbb{F}_{p^2}, \mathcal{O}) \\ (E, [\mathfrak{a}]) & \mapsto & [\mathfrak{a}] \cdot E = E/E[\mathfrak{a}] \end{array}$$

Definition 2.2 *We define a vortex to be the l-isogeny graph whose vertices are isomorphism classes of $\mathcal{O}$-oriented supersingular elliptic curves with l-maximal endomorphism ring, equiped with an action of $Cl(\mathcal{O})$.*

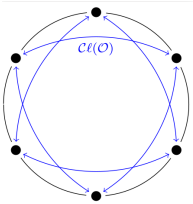


Figure 1: Example of a *vortex* under the action of $Cl(\mathcal{O}$

The action of $Cl(\mathcal{O})$ extends to the union $\cup_i SSO(\mathbb{F}_{p^2}, \mathcal{O}_i)$ over all superorders $\mathcal{O}_i$ containing $\mathcal{O}$ via the surjections $\mathcal{O}_i$.

Definition 2.3 *We define a whirpool to be an l-isogeny graph of $\mathcal{O}$-oriented supersingular elliptic curves acted on by $Cl(\mathcal{O})$.*

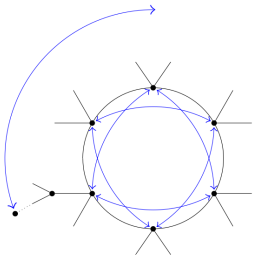


Figure 2: Example of a *whirpool* under the action of $Cl(\mathcal{O}$

3 l-ladders

Let's consider a descending l-isogeny chain (E_i, ϕ_i) of $\mathcal{O}$-oriented supersingular elliptic curves with

$$\mathcal{O}_K \subset End(E_0), \cdots, \mathcal{O} = \mathbb{Z} + l^n\mathcal{O}_K \subset End(E_n).$$

Fix $\mathfrak{q}$ a prime in $\mathcal{O}_K$ over a small prime number q ($q \neq l, p$) that splits in $\mathcal{O}_K$. Then the isogeny

$$\psi_0 : E_0 \to F_0 = E_0/E_0[\mathfrak{q}]$$

can be extended to the l-isogeny chain by pushing forward the cyclic group $C_0 = E_0[\mathfrak{q}]$:

$$C_1 = \phi_0(C_0), \cdots, C_n = \phi_{n-1}(C_{n-1}),$$

and defining $F_i = E_i/C_i$. This construction motivates the following definitions.

Definition 3.1 *An l-ladder of length n and degree q is a commutative diagram of l-isogeny chains (E_i, ϕ_i) and (F_i, ϕ'_i) of lenght n connected by q-isogenies $\psi_i : E_i \to F_i$.*

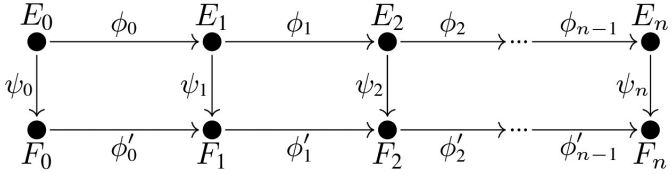


Figure 3: Example of an l-ladder

Considering modular polynomials $\Phi_m(X, Y) \in \mathbb{Z}[X, Y]$, there exist a cyclic m-isogeny between two curves E and E' if and only if $\Phi_m(j(E), j(E')) = 0$.

Definition 3.2 *A modular l-isogeny chain of length n over k is a finite sequence $(j_0, j_1, \cdots, j_n)$ in k such that $\Phi_l(j_i, j_{i+1}) = 0$ for $0 \leq i < n$. A modular l-ladder of length n and degree q is a pair of modular l-isogeny chains*

$$(j_0, j_1, \cdots, j_n) \text{ and } (j'_0, j'_1, \cdots, j'_n) \text{ such that } \Phi_q(j_i, j'_i) = 0$$

Clearly, an l-isogeny chain (E_i, ϕ_i) determines the modular l-isogeny chain $(j_i = j(E_i))$, and the converse is also true.
Given any modular l-isogeny chain (j_i), a supersingular elliptic curve E_0 with $j(E_0) = j_0$, and an q-isogeny $\psi_0 : E_0 \to F_0$, it follows that we can construct an l-ladder $\psi : (E_i, \phi_i) \to (F_i, \phi'_i)$ and hence a modular l-ladder. In fact the l-ladder can be efficiently constructed recursively from the l-isogeny chains $(j_0, \cdots, j_n)$ and $(j'_0, \cdots, j'_i)$, by solving the system of equations

$$\begin{cases} \Phi_l(j'_i, Y) = 0 \\ \Phi_q(j_{i+1}, Y) = 0 \end{cases}$$

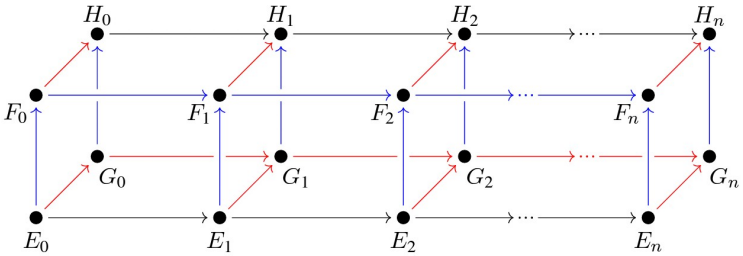
4 OSIDH

We now describe a general construction for a key exchange protocol using oriented supersingular elliptic curves. The first protocol is a naive construction that serves as a bridge to the second one which is better secured.
For the general setting, let $\mathcal{O}_K$, of class number 1, be the maximal order of an imaginary quadratic field K; and p a large prime such that $\left(\frac{\Delta_K}{p}\right) \neq 1$.
Alice and Bob agree on an $\mathcal{O}_K-$oriented supersingular elliptic curve $E_0/\mathbb{F}_{p^2}$, a small prime l and a descending isogeny chain

$$E_0 \longrightarrow E_1 \longrightarrow E_2 \longrightarrow \cdots \longrightarrow E_n$$

Alice chooses a horizontal endomorphism $\psi_A = \psi_0 : E_0 \to F_0 = E_0$ and pushes it foward to an $l-$ladder of lenght n.

The $l-$isogeny chain (F_i) is sent to Bob. Bob chosses an endomorphism ψ_B and sends the resulting $l-$isogeny chain (G_i) to Alice. Each applies the private endomorphism to obtain $(H_i) = \psi_A \cdot (G_i) = \psi_B \cdot (F_i)$, and $H = H_n$ is the shared secret. This protocol is resumed in the following picture. The blue arrows correspond to the orientation chosen throughout by Alice while the red ones represent the choice made by Bob.



This naive protocol presents some week points. Firstly, we know $End(E_0)$ and pushing forward the $l-$ladder (from a descending isogeny chain) implies $\mathbb{Z} + l^n End(E_0) \subset End(E_n) = End(H_n) = End(H)$. Using the following theorem, one may be able to construct ψ_A.

Theorem 4.1 *([4]) Let E and E_A be supersingular elliptic curves over $\mathbb{F}_{p^2}$ such that $E[l^n] \subset E(\mathbb{F}_{p^2})$ and there is an isogeny $\psi_A : E \to E_A$ of degree l^n. Suppose there is no isogeny $\phi : E \to E_A$ of degree strictly less thant l^n. Then, given an explicit description of $End(E)$ and $End(E_A)$, there is an efficient algorithm to compute ψ_A.*

Secondly, sharing (F_i) and (G_i) reveals too much of private data. From the exact short sequence of class groups:

$$1 \to \frac{(\mathcal{O}_K/l^n\mathcal{O}_K)^\times}{\overline{\mathcal{O}}_K^\times(\mathbb{Z}/l^n\mathbb{Z})^\times} \to Cl(\mathcal{O}) \to Cl(\mathcal{O}_K) \to 1,$$

an adversary can compute successive approximations (mod l^i) to ψ_A and ψ_B modulo l^n hence in $Cl(\mathcal{O})$. You can find more details in [3].

We refine the protocol as follows.
A set of prime ideals $\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_t \subset \mathcal{O} = \mathcal{O}_n = End(E_n) \cap K \hookrightarrow \mathcal{O}_K$ (respectively over primes $p_1, p_2, \cdots, p_t$ that split in $\mathcal{O}$) and a positive integer r such that $(2r+1)^t \approx \lceil \frac{p}{12} \rceil$ are added to the previous public parameters.
Alice chooses a tuple of integers $(e_1, \cdots, e_t) \in [-r, r]^t$ and constructs an isogenous curve $F_n = \frac{E_n}{E_n[\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_t^{e_t}]}$. She also computes for each i, the horizontal isogeny chains determined by the isogenies with kernel $F_n[\mathfrak{p}_i^j]$ for $j \in [-r, r]$ and $\mathfrak{p}_i^{-j} := \overline{\mathfrak{p}_i}^{-j}$. She sends F_n and the isogeny chains to Bob. Bob does the same with a tuple $(d_1, \cdots, d_t)$ and sends the curve G_n and the coresponding isogeny chains to Alice. Alice Takes e_i steps in the p_i-isogeny chain and pushes foward the information for all $j > i$ and Bob does the same.

Both of them share the same elliptic cure

$$H_n = \frac{F_n}{F_n[\mathfrak{p}_1^{d_1} \cdots \mathfrak{p}_t^{d_t}]} = \frac{G_n}{G_n[\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_t^{e_t}]} = \frac{E_n}{E_n[\mathfrak{p}_1^{e_1+d_1} \cdots \mathfrak{p}_t^{e_t+d_t}]}$$

This scheme is resumed in the following picture.

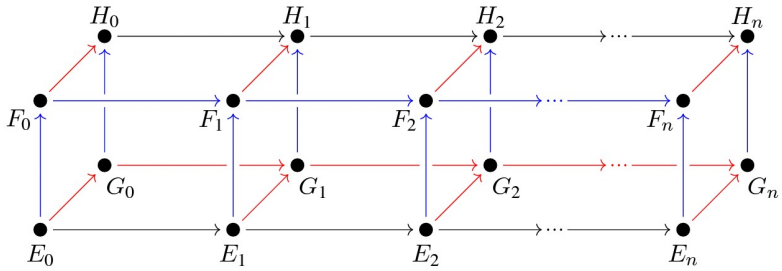


Figure 4: Graphic representation of OSIDH

References

[1] W. Castryck, T. Lange, C. Martindale, L. Panny, and J. Renes, *CSIDH: an efficient post-quantum commutative group action*, In Advances in Cryptology - ASIACRYPT 2018, Lecture Notes in Computer Science, vol 11274, Springer, 2018.

[2] D. Charles, E. Goren, and C. Lauter, *Cryptographic hash functions from expandergraphs*, J. Cryptography 22 (1), 93–113, 2009.

[3] L. Colò and D. Kohel, *Orienting supersingular isogeny graphs*, http://nutmic2019.imj-prg.fr/confpapers/OrientIsogGraph.pdf.

[4] S.D. Galbraith, C. Petit, B. Shani and Y.B. Ti., *On the Security of Supersingular Isogeny Cryptosystems*, In ASIACRYPT

(1), Springer, 63-91, 2016. https://eprint.iacr.org/2016/859.

[5] D. Jao and L. De Feo, *Towards quantum-resistant cryptosystems from supersin-gular elliptic curve isogenies*, In Post-Quantum Cryptography, LNCS 7071, 19–34, Springer, 2011. https://eprint.iacr.org/2011/506.

Boris Fouotsa Tako
Department of Mathematics and Physics
Roma Tre University
Email: takoboris.fouotsa@uniroma3.it

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 5, *Number* 1, *March* 2020, *pages* 51-58

Pär Kurlberg

Prime and Möbius correlations for very short intervals in $\mathbb{F}_p[X]$.

Written by Oussama Rayen Hamza

Introduction

Pär Kurlberg gave a talk the $19th$ April 2019 about the two articles, written by P. Kurlberg and L. Rosenzweig : "Prime and Möbius correlations for very short intervals in $\mathbb{F}_q[x]$" [1]; and " The Chebotarev density theorem for function fields, incomplete intervals", [2].
We give the abstract of this talk, written by P. Kurlberg:
"We investigate function field analogs of the distribution of primes, and prime k-tuples, in "very short intervals "of the form $I(f) := \{f(x) + a : a \in \mathbb{F}_p\}$ for $f(x) \in \mathbb{F}_p[x]$ and p prime, as well as cancellation in sums of function field analogs of the Möbius function and its correlations (similar to sums appearing in Chowla's conjecture). For generic f, i.e., for f a "t Morse polynomial" , we show that error terms are roughly of size $O(\sqrt{p})$ (with typical main terms of order p). We also give examples of f for which there is no cancellation at all, and intervals where the heuristic "primes are independent" fails very badly. Time permitting we will discuss the curios fact that (square root) cancellation in Möbius sums is "equivalent" to (square root) cancellation in Chowla type sums.
"

1 Some prerequisites and study of intervals in $\mathbb{F}_p[x]$.

We will first show some analogies between $\mathbb{Z}$ and the ring $\mathbb{F}_p[x]$:

$$\mathbb{Z} \longleftrightarrow \mathbb{F}_p[x]$$

$$\text{prime numbers} \longleftrightarrow \text{irreducible polynomials in } \mathbb{F}_p[x]$$

$$\text{size of } n = |n| = |\mathbb{Z}/n\mathbb{Z}| \longleftrightarrow \text{size of } f = |f| = |\mathbb{F}_p[x]/(f)| = p^{\deg(f)}$$

So, we can define the Möbius function μ in $\mathbb{F}_p[x]$ analogously to the usual Möbius function in $\mathbb{Z}$: let f an element in $\mathbb{F}_p[x]$; if f is not squarefree, then we set $\mu(f) = 0$, else we can write $f = g_1 \dots g_n$, as a product of n distinct prime factors, and we set $\mu(g) = (-1)^n$.

Now, let d be an integer, we define $M_d(\mathbb{F}_p[x]) = \{g \in \mathbb{F}_p[x]; \deg(g) = d \text{ and } g \text{ is monic }\}$, we can see this set as an interval in $\mathbb{F}_p[x]$. We have the following results about the repartitions of irreducible polynomials into these intervals:

Theorem 1 (Gauss 1828) *We have:*

$$|\{f \in M_d(\mathbb{F}_p[x]); f \text{ is irreducible }\}| = \frac{1}{d}\sum_{e|d}\mu(d/e)p^e = \frac{p}{d} + O(p^{d/2}).$$

We say here that the prime density of $M_d(\mathbb{F}_p[x])$ is $1/d$.

We want now to generalise this result to shorter intervals. So we begin to define shorter ones :

$$I(f; m) = \{f + \sum_{i=0}^{m} a_i x^i; a_0, \dots, a_m \in \mathbb{F}_p\}.$$

We are in particular interested in very short intervals of the shape:

$$I(f) = I(f;0) = \{f + a; a \in \mathbb{F}_p\} = \{g \in \mathbb{F}_p[x]; |g - f| \leq 1\}.$$

However, to obtain similar result as the theorem 1, f has to satisfy some conditions:

Definition 1 *The polynomial $f \in M_d(\mathbb{F}_p[x])$ is Morse if and only if f has $d-1$ critical values, i.e.:*

$$|\{f(\zeta); f'(\zeta) = 0\}| = d - 1.$$

Example 1 *The polynomials $x, x^2, x(x^2-1)$ are Morse. However, the polynomials $x^3, x^4(x^2-1)$ are not Morse.*

Remark 1

1. *If $f \in M_d(\mathbb{F}_p[x])$, then we have:*

$$|\{s \in \mathbb{F}_p; f + s.x \text{ is Morse }\}| = p + O_d(1).$$

2. *And thanks to Hilbert's theorem, if $g \in \mathbb{Q}[x]$ is of degree d and Morse, then g has a nice Galois Group, i.e.:*

$$Gal(f(x) + t/\mathbb{Q}(t)) = S_d.$$

We finally obtain this result, from the article [1], as a generalisation of theorem 1:

Theorem 2 *If $f \in M_d(\mathbb{F}_p[x])$ is Morse, then we have:*

$$|\{g \in I(f); g \text{ is prime }\}| = \frac{1}{d}p + O_d(\sqrt{p}). \quad (1)$$

We say that the prime density of $I(f)$ is $1/d$.
Moreover, for distinct $h_1; \ldots; h_k \in \mathbb{F}_p$, we have:

$$|\{g \in I(f); g+h_1, \ldots, g+h_k \text{ are all primes }\}| = (\frac{1}{d})^k.p + O_{d;k}(\sqrt{p}). \quad (2)$$

In general, this theorem is not true, when we take f not Morse, we will give some examples:

Example 2 *1. Assume* $p \equiv 2 \mod 3$ *and take* $f = x^3$*, then:*

$$|\{a \in \mathbb{F}_p; x^3 + a \text{ is irreducible }\}| = 0.$$

So the prime density of $I(f)$ *is* 0.
Assume now that $p \equiv 2 \mod 3$*, then*

$$|\{a \in \mathbb{F}_p; x^3 + a \text{ is prime }\}| = \frac{2}{3}p + O(\sqrt{p}).$$

The prime density is twice the expected density.

2. Now take $f = x^4 - 2x^2$ $(d = 4)$*, then we have*

$$|\{a \in \mathbb{F}_p; a + f(x) \text{ is prime }\}| = \frac{1}{4}p + O(\sqrt{p}).$$

We also have the same result, when we replace f *by* $f + 1$.
However:

$$|\{a \in \mathbb{F}_p; f(x) + a, f(x) + a + 1 \text{ are both primes }\}| = O(\sqrt{p}),$$

when $p \equiv 3 \mod 4$*, and*

$$|\{a \in \mathbb{F}_p; f(x)+a, f(x)+a+1 \text{ are both primes }\}| = \frac{1}{8}p+O(\sqrt{p}),$$

when $p \equiv 1 \mod 4$.

Remark 2 (Related work) *We assume that the polynomial* f *satisfies the hypotheses of the theorem* 2.

- *Bank, Bary-Soroker and Rosenzweig have shown in the article [3], that: the equality* (1) *is true if* $(p; 2d(d-1)) = 1$*, for* $I(f, 1)$*. This equality is also true for* $I(f, 2)$ *assuming some other conditions.*

- *Pollack has also shown, in 2008, that the equality* (2) *is true for* $I = M_d(\mathbb{F}_p[x]$*, for* $(2d; p) = 1$.
  After, in 2014, Bary-Soroker showed that this equality is also true if $(2d; q) > 1$.

2 Cancellation in Möbius and Chowla type sums for function fields

In this part, we will see some results about the Möbius μ function for function fields.

Theorem 3 *Assume $f \in M_d(\mathbb{F}_p)$ is Morse, then we have:*

1.
$$\sum_{g \in I(f)} \mu(g) = O_d(\sqrt{p}),$$

2. *Moreover, take k elements $h_1; \ldots; h_k \in \mathbb{F}_p$, then we have:*
$$\sum_{g \in I(f)} \mu(g + h_1) \ldots \mu(g + h_k) = O_{d;k}(\sqrt{p})$$

In fact, for any $f \in M_d(\mathbb{F}_p)$ (without the Morse assumption), we have $1 \iff 2$.

Example 3 *If $p \equiv 2 \mod 3$, and we assume that $f = x^3$, then we have:*
$$\sum_{g \in I(x^3)} \mu(g) = p + O(1).$$

Remark 3 (Related work) *We assume that the polynomial f satisfies the hypotheses of the theorem* 3.

- *Carmon-Rudnik have shown that the equality* 2 *and* 1 *are true for $I = M_d(\mathbb{F}_p[x])$, in the article [4].*
- *Keating-Rudnik have shown, in the article [5], that the equality* 1 *is also true for $I = I(f; m)$ if $m \geq 2$.*

Finally, we remind a theorem, from the article [6]:

Theorem 4 (Shparlinski) *Assume I_0, I_1 two intervals in $\mathbb{N}$, such that for some $\varepsilon > 0$, we have :*

$$|I_0|, |I_1| > p^{1/4+\varepsilon} \text{ and } |I_0||I_1| > p^{1+\varepsilon}.$$

Then, we obtain:

$$|\{(a_0; a_1) \in I_0 \times I_1; x^d + a_1 x + a_0 \text{ is irreducible } \}| \sim \frac{|I_0||I_1|}{d}.$$

Rosenzweig and Kurlberg obtain a stronger form of this theorem: they assume weaker properties on I_0, I_1, and obtain the same result.

Theorem 5 *Assume I_0, I_1 two intervals in $\mathbb{N}$, such that we have :*

$$|I_0|^{-1} = o(1) \text{ and } p^{1/2}/|I_1| = o(1).$$

Then, we obtain:

$$|\{(a_0; a_1) \in I_0 \times I_1; x^d + a_1 x + a_0 \text{ is irreducible } \}| \sim \frac{|I_0||I_1|}{d}.$$

3 Galois theory

We assume $f \in M_d(\mathbb{F}_p)$, so the polynomial $g_t(x) = f(x) + t \in \mathbb{F}_p(t)[x]$ is irreducible, so consequently, we put $K/\mathbb{F}_p(t)$ the splitting field of f, and L/K its Galois closure:

$$\mathbb{F}_p(t) \subset K \subset L.$$

We also put $G = Gal(L/\mathbb{F}_p(t))$.
The aim of this part is to compute the prime density of $I(f)$, i.e.:

$$|\{a \in \mathbb{F}_p; f(x) + a = g_t(x) - (t - a) \text{ is prime } \}|.$$

Remark 4 *Let $p_a = (t - a)$ an ideal of $\mathbb{F}_p(t)$, then we define*

$$\sigma_a = (\frac{L/\mathbb{F}_p(t)}{p_a}) \subset G$$

as the Artin Symbol of p_a in L (this is a conjugacy class in G).
Then every element of σ_a is a d-cycle, if and only if $f(x) + a = g_t(x) - (t - a)$ is prime in $\mathbb{F}_p(t)[x]$.
For more details, we can see the part 6*, chapter* 7 *of* [8].

So we can conclude with this theorem:

Theorem 6 (Reichardt, Cohen-Odoni, Jarden, Fried) *Let $C \subset G$ be a conjugacy class, and assume moreover, $L \cap \overline{\mathbb{F}_p} = \mathbb{F}_p$.*
Then, we have: $|\{a; \in \mathbb{F}_p; \sigma_a \in C\}| = \frac{|C|}{|G|}p + O_{[L:\mathbb{F}_p(t)]}(\sqrt{p})$.

So now suppose that f is Morse. Thanks to Hilbert's Theorem: $G = S_d$. So put $C = \{\sigma; \sigma$ is a d-cycle $\} \subset G$, this is a conjugacy class of cardinality $(d-1)!$.
So we get $\frac{|C|}{|G|} = \frac{1}{d}$, and finally:

$$|\{a \in \mathbb{F}_p; f(x) + a \text{ is a prime } \}| = \frac{p}{d} + O(\sqrt{p}).$$

So the prime density of $I(f)$ is $\frac{1}{d}$.

Now, let $h_1 \neq h_2$ both in $\mathbb{F}_p$.
We want to compute $|\{a \in \mathbb{F}_p; f(x)+a+h_1$ and $f(x)+a+h_2$ both primes $\}|$.
So we put $K_{h_i}/\mathbb{F}_p(t)$ the splitting field of $g_t(x) + h_i$ in $\mathbb{F}_p(t)$, and we put L_{h_i}/K_{h_i} the Galois closure of K_{h_i}. We finally put $G_{h_i} = Gal(L_{h_i}/\mathbb{F}_p(t))$.
Now, remark that if f is Morse, then by definition, $f + h_i$ is also Morse.
So we get $G_{h_1} = G_{h_2} = S_d$.
So now, put $L^2 = L_{h_1}L_{h_2}$, if p is big enough, then we get

$$G^2 = Gal(L^2/\mathbb{F}_p(t)) \simeq S_d \times S_d.$$

Finally, we can prove, that we have a prime density of $\frac{1}{d}.\frac{1}{d}$, ie:

$$|\{a; \in \mathbb{F}_p; f(x)+a+h_1 \text{ and } f(x)+a+h_2 \text{ both prime } \}| = \frac{1}{d^2}p + O(\sqrt{p}).$$

References

[1] P. Kurlberg and L. Rosenzweig, *Prime and Möbius correlations for very short intervals in $\mathbb{F}_q[x]$*. 2019

[2] P.Kurlberg and L. Rosenzweig, *The Chebotarev density theorem for function fields; incomplete intervals*. 2019

[3] E. Bank, L. Bary-Soroker, and L. Rosenzweig, *Prime polynomials in short intervals and in arithmetic progressions*. Duke Math. J., **164(2)** (2015), 277–295

[4] D. Carmon and Z. Rudnick, *The autocorrelation of the Möbius function and Chowla's conjecture for the rational function field*. Q. J. Math., **65(1)** (2014), 53–61

[5] J. Keating and Z. Rudnick, *Squarefree polynomials and Möbius values in short intervals and arithmetic progressions*. Algebra Number Theory, **10(2)** (2016), 375–420

[6] I. E. Shparlinski, *On the distribution of irreducible trinomials*. Canad. Math.Bull., **54(4)** (2011) 748–756

[7] H. Reichardt. *Der Primdivisorsatz für algebraische Funktionen korper uber einem endlichen Konstanten korper*. Math. Z., **40(1)** (1936), 713–719

[8] J. Neukirch, *Algebraic Number Theory*. Springer, Berlin, 1999.

Oussama Hamza
Mathematics
Ecole Normale superieure de Lyon
15 parvis Rene Descartes
69342 Lyon France.
email: oussama.hamza@ens-lyon.fr

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 5, *Number* 1, *March* 2020, *pages* 59-65

David Masser

On Siegel's Lemma

Written by Guido Lido

1 Diophantine approximation and linear systems

In 1844 Liouville proved that, if $\alpha \in \mathbb{R}$ is algebraic of degree $d \geq 2$, then there exists a constant $c > 0$, depending on α, such that for each choice of $p \in \mathbb{Z}$ and $q \in \mathbb{Z}_{>0}$

$$\left|\alpha - \frac{p}{q}\right| > c\frac{1}{q^d}\,.$$

This result has been successively sharpened during the 20^{th} century, for example by Thue and Siegel who proved the following theorems.

Theorem 1 (Thue, 1909) *Let $\alpha \in \mathbb{R}$ be an algebraic number of degree $d \geq 3$. Then for each*

$$\kappa > \frac{d}{2} + 1$$

there exists a constant $c > 0$, depending on α and κ such that, for each choice of $p \in \mathbb{Z}$ and $q \in \mathbb{Z}_{>0}$, we have

$$\left|\alpha - \frac{p}{q}\right| > c\frac{1}{q^\kappa}\,.$$

Theorem 2 (Siegel, 1921) *Let $\alpha \in \mathbb{R}$ be an algebraic number of degree $d \geq 3$. Then for each*

$$\kappa > \min_{\delta=1,\ldots,d} \left(\delta + \frac{d}{\delta + 1} \right)$$

there exists a constant $c > 0$, depending on α and κ, such that for each choice of $p \in \mathbb{Z}$ and $q \in \mathbb{Z}_{>0}$

$$\left| \alpha - \frac{p}{q} \right| > c \frac{1}{q^\kappa} .$$

In particular this is true for each $\kappa > 2\sqrt{d}$.

A common strategy in the original proofs of both theorems is to use a "good" approximation of α to construct a non-trivial polynomial in several variables with small integer coefficients and many zeroes and then deriving a contradiction. The construction of such a polynomial is a matter of linear algebra over the integers: in [4] Siegel isolated the idea behind this part of the proof in a lemma popularly known as "Siegels's Lemma"

2 Siegel's Lemma: ideas of proof and generalizations

Lemma 1 (Siegel, 1929) *Let $M < N$ be positive integers, let $U \geq 1$ be a real number and let $u = (u_{mn}) \in \mathbb{Z}^{M \times N}$ be a matrix with entries of absolute value at most U. Then the linear system*

$$\begin{cases} u_{11}x_1 + \ldots + u_{1N}x_N = 0 \\ \vdots \\ u_{M1}x_1 + \ldots + u_{MN}x_N = 0 \end{cases}$$

admits a non-zero solution $(x_i) \in \mathbb{Z}^N$ satisfying

$$\max_{i=1,\ldots,N} |x_i| \leq (NU)^{\frac{M}{N-M}} .$$

Notice that the theorem would be false if we took $U < 1/N$, thus the hypothesis $U \geq 1$ cannot be simply removed: it is funny to say that Siegel himself had to remark it during the lectures of other (now famous) mathematicians.

Instead of giving a complete proof of the above Lemma, let us only consider the cases $N = 3$. If $N = 3$ and $M = 1$ we can prove the theorem using the pigeonhole principle. Let us see the matrix (u_{mn}) as a linear map $u\colon \mathbb{R}^3 \to \mathbb{R}$. Let $\lambda = \lfloor \sqrt{3U} \rfloor$ and let us consider the image of $I = \{0, \dots, \lambda\}^3$ under u: if $\xi = (\lambda/2, \lambda/2, \lambda/2)$ then, for each $x = (x_1, x_2, x_3) \in I$, we would have

$$|u(x) - u(\xi)| = |u_{11}(x_1 - \lambda/2) + u_{12}(x_2 - \lambda/2) + u_{13}(x_3 - \lambda/2)| \leq \frac{3}{2}\lambda U\,.$$

Thus, as x varies in I the vector $u(x)$ is an integer varying in an interval of length $3\lambda U$, i.e., $u(x)$ varies in a set J of size at most $3\lambda U + 1$. Since $\#J \leq 3(\lambda+1)U < (\lambda+1)^3 = \#I$ we conclude that there exist $x' \neq x'' \in I$ such that $u(x') = u(x'')$. Thus the vector $x = (x_1, x_2, x_3) := x' - x''$ is non-zero and satisfies

$$\max_{i=1,2,3} |x_i| \leq \lambda \leq \sqrt{3U}\,, \quad u(x) = 0\,.$$

If $N = 3$, $M = 2$ and the matrix (u_{mn}) has rank 1 we can deduce the thesis from the case $N = 3, M = 1$, while if the matrix (u_{mn}) has rank 2 then we can just take

$$x_1 = u_{12}u_{23} - u_{13}u_{22}\,, \quad x_2 = u_{13}u_{21} - u_{11}u_{23}\,, \quad x_3 = u_{11}u_{22} - u_{12}u_{21} \tag{1}$$

and this solution satisfies $\max_{i=1,2,3} |x_i| \leq 2U^2 \leq (3U)^2$.

A full proof of the Lemma can be done using the pigeonhole principle in a similar manner to the case $N = 3, M = 1$ or using techniques from Geometry of Numbers.

Several improvements and generalizations of Siegel's Lemma have been formulated. For example in [5] a generalization valid for function fields is proven and [1] contains a version for number fields.

In particular, given two positive integers $M < N$, a number field K and a matrix $u \in K^{M\times N}$ of rank M, Bombieri and Vaaler define a height $H(u)$ (playing the role of the real number U) and prove the existence of a non-zero solution $x \in K^N$ with multiplicative height

$$H(x) \leq \left(\frac{2^s}{\pi^s}\sqrt{|\Delta_K|}\right)^{\frac{1}{[K:\mathbb{Q}]}} H(u)^{\frac{1}{N-M}}$$

where s is the number of complex embeddings of K and Δ_K is the discriminant of K.

3 Sharpness of the Lemma

A natural (vague) question to ask is how sharp Siegel's Lemma is.

A first answer has been given by W.M. Schmidt who proved that the exponent in the Lemma is best possible. Indeed, in the first pages of [3], for each pair of positive integers $M < N$ and for each $\epsilon > 0$, Schmidt constructs an infinite family of linear systems $(u_{mn}) \in \mathbb{Z}^{M\times N}$ with the property that each non-zero solution $(x_i) \in \mathbb{Z}^N$ satisfies

$$\max_{i=1,\ldots,N} |x_i| > (1-\epsilon) \max_{\substack{m=1,\ldots,M \\ n=1,\ldots N}} |u_{m,n}|^{\frac{M}{N-M}} .$$

This shows that for each choice of a constant $c_{N,M}$ and for each choice of a function $f_{N,M} : \mathbb{R}_{>0} \to \mathbb{R}_{>0}$ such that, for large U, one has $f_{N,M}(U) = o(U^{\frac{M}{N-M}})$, Siegel's Lemma becomes *false* if we impose

$$\max_{i=1,\ldots,N} |x_i| \leq c_{N,M} f_{N,M}(U) \quad \text{instead of} \quad \max_{i=1,\ldots,N} |x_i| \leq (NU)^{\frac{M}{N-M}} .$$

In particular, for each $\epsilon > 0$, Siegel's Lemma becomes false if we impose $\max |x_i| \leq c_{N,M} U^{\frac{M}{N-M}-\epsilon}$.

Another result about the sharpness of Siegel's Lemma has been given by Beck in [2] and it is more concerned with the constant $c_{N,M}$. In

particular in [6] one can find a version of Lemma 1 stating that, with the same hypotheses, there exists a solution $x = (x_i) \in \mathbb{Z}^N$ satisfying

$$\max_{i=1,\dots,N} |x_i| \leq \left(\sqrt{N+1}\, U\right)^{\frac{M}{N-M}} .$$

In 2017 Beck proved that there exists a (small) constant $c_0 > 0$ such that, for each positive integers $N \geq \frac{3}{2}M$, there exists a linear system (u_{mn}) with coefficients $u_{mn} \in \{\pm 1\}$ such that every solution satisfies

$$\max_{i=1,\dots,N} |x_i| > c_0(\sqrt{N})^{\frac{M}{N-M}} . \tag{2}$$

In [2] it is actually proven that, choosing $c_0 = 10^{-30}$, all but a small proportion (i.e. $O(2^{-M/2})$) of all systems with coefficients in $\{\pm 1\}$ has big solutions in the sense of equation (2). The proof is not constructive and uses Fourier analysis and Erdös's probabilistic method.

The last result about the sharpness of Siegel's lemma is a recent work by David Masser and Roger Baker proving that the Lemma is sharp "in most cases" in the following sense.

Theorem 3 *[David Masser, Roger Baker] Let $M < N$ be positive integers. There exist constants $C, \theta > 0$ depending on N with the following property: for any pair of real numbers $U, B \geq 1$ there are at most*

$$\frac{CU^{MN}}{B^{\theta}}$$

systems $(u_{mn}) \in \mathbb{Z}^{M\times N}$ such that $|u_{mn}| \leq U$ and such that some non trivial solution $(x_i) \in \mathbb{Z}^N$ satisfies

$$\max_{i=1,\dots,N} |x_i| < \frac{U^{\frac{M}{N-M}}}{B} .$$

For example this theorem implies that for each function $f\colon \mathbb{R}_{>0} \to \mathbb{R}_{>0}$ such that, for large U, one has $f(U) = o(U^{\frac{M}{N-M}})$ then, among all the systems $(u_{mn})^{M\times N}$ with absolute value of the coefficients at most U,

the proportion of systems admitting a non zero solution $(x_i) \in \mathbb{Z}^N$ satisfying $\max |x_i| \leq f(U)$ is a proportion tending to zero as U tends to infinity.

The proof of Theorem 3 becomes more difficult when M and N get near. For example in the cases where $N \geq 2M$ Theorem 3 can be proved using Widmer's techniques for counting intersections of lattices and constructible regions of Euclidean spaces. If one wants to treat more cases i.e. when $N \geq M + 2$ then these techniques are not enough anymore but W.M. Schmidt's heights of subspaces comes to help. The cases $N = M + 1$ is the most difficult, which is paradoxical as then there are usually explicit solutions like (1).

References

[1] E. Bombieri and J. Vaaler, *On Siegel's lemma*. Invent. Math. **73.1** (1983), 11-32.

[2] J. Beck, *Siegel's Lemma is sharp*. In: *A Journey Through Discrete Mathematics*, 165-206, Springer, Cham, 2017.

[3] W. M. Schmidt, *Diophantine Approximations and Diophantine Equations*. Springer, Berlin, Heidelberg, 1991.

[4] C.L. Siegel, *Uber einige Anwendungen Diophantischer Approximationen*. 209âĂŞ266, Abh. Preuss. Akad. Wiss. Phys. Math., 1929.

[5] J. L. Thunder, *Siegel's lemma for function fields*. The Michigan Math. Jour. **42.1** (1995), 147-162.

[6] J. Vaaler and A. Van der Poorten, *Bounds for solutions of systems of linear equations*. Bull. Austr. Math. Soc. **25.1** (1982), 125-132.

Guido Maria Lido
Department of Mathematics
University of Rome Tor Vergata
Via della Ricerca Scientifica 1
00133 Roma, Italy.
email: guidomaria.lido@gmail.com

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 5, *Number* 1, *March* 2020, *pages* 67-79

Florian Luca

Coordinates of Pell equations in various sequences

Written by Andam Mustafa

Let d be a positive integer which is not a square. The Pell equation corresponding to d is the equation

$$X^2 - dY^2 = \pm 1 \tag{1}$$

to be solved in positive integers (X, Y).

It is known that (1) always has positive integer solutions. Letting (X_1, Y_1) be the smaller positive integer solution of it, all other solutions are of the form (X_n, Y_n) with

$$X_n + \sqrt{d}Y_n = (X_1 + \sqrt{d}Y_1)^n \quad \text{for all} \quad n \geq 1.$$

First attempt of the problem by letting $\mathcal{U}$ be your favorite set of positive integers. What can one say about d such that the equation

$$X_n \in \mathcal{U} \quad \text{for some} \quad n? \tag{2}$$

Unfortunately, if one formulates it in this way, the above problem is trivial. Indeed, $u \in \mathcal{U}$ and write

$$u^2 + 1 = dv^2,$$

for some squarefree integer d. Then

$$u^2 - dv^2 = -1,$$

so $u = X_n$ for some $n \geq 1$ corresponding to d. If $u > 1$, we can play the same game with

$$u^2 - 1 = dv^2.$$

Now, we try a second attempt of our problem. Since our first attempt seemed to have a trivial answer, we try the following potentially more interesting problem: What can we say about d such that

$$X_n \in \mathcal{U}$$

holds for at least two different values of n? That is, we now look for values of the squarefree integer d such that the equation

$$U^2 - dV^2 = \pm 1,$$

has two different positive integer solutions $(U, V) \neq (U', V')$ with $\{U, U'\} \subset \mathcal{U}$. Let us look at a few examples:
Take

$$\mathcal{U} = \left\{ a\left(\frac{10^m - 1}{9}\right); 1 \leq a \leq 9,\ m \geq 1 \right\}.$$

The elements of $\mathcal{U}$ are base 10 repdigits since

$$a\left(\frac{10^m - 1}{9}\right) = \underbrace{\overline{aa\cdots a}}_{m \text{ times}}.$$

Theorem 1 (A. Dossavi-Yovo, F. Luca and A. Togbé, 2016.) *Let (X_n, Y_n) be the nth solution of the Diophantine equation*

$$X^2 - dY^2 = 1.$$

The equation $X_n \in \mathcal{U}$ has at most one solution n except:

(i) $d = 2$ *for which* $n \in \{1, 3\}$,

(ii) $d = 3$ *for which* $n \in \{1, 2\}$.

Now let $\mathcal{U}$ be the sequence of all Fibonacci numbers given by $F_1 = F_2 = 1$ and $F_{n+2} = F_{n+1} + F_n$ for all $n \geq 1$.

Theorem 2 (F. Luca and A. Togbé, 2018.) *Let* (X_n, Y_n) *be the nth solution of the Diophantine equation*

$$X^2 - dY^2 = \pm 1$$

The equation $X_n \in \mathcal{U}$ *has at most one solution n except for* $d = 2$ *in which case* $n \in \{1, 2\}$.

The above result can be reformulated by saying that the only nontrivial solutions of the Diophantine equation

$$(F_n^2 \pm 1)(F_m^2 \pm 1) = \square$$

are $(n, m) = (1, 4),\ (2, 4)$.
Let $g \geq 2$ be an integer and

$$\mathcal{U}_g = \left\{ a\left(\frac{g^m - 1}{g - 1}\right); 1 \leq a \leq g - 1,\ m \geq 1 \right\}.$$

The members of $\mathcal{U}_g$ are called base g-repdigits.

Theorem 3 (B. Faye and F. Luca, 2016.) *Let* (X_n, Y_n) *be the nth solution of the Diophantine equation*

$$X^2 - dY^2 = 1.$$

If $X_n \in \mathcal{U}$ *has two solutions n, then*

$$d < \exp\left((10g)^{10^5}\right).$$

Next, we take $\mathcal{U} = \{F_n : n \geq 4\}$.

Theorem 4 (B. Kafle, F. Luca and A. Togbé, 2018.) *Let* (X_n, Y_n) *be the nth solution of the Diophantine equation*

$$X^2 - dY^2 = \pm 4. \tag{3}$$

The equation $X_n \in \mathcal{U}$ *has at most one solution n.*

Allowing also the "small Fibonacci numbers", we get that the equation $X_n \in \mathcal{U}$, where (X_n, Y_n) satisfies (8) has only one solution n except when $d \in \{2, 5\}$ for which all n have $n \leq 4$.

Let $\mathcal{U}$ be the sequence of Tribonacci numbers which is given by $T_1 = T_2 = 1$, $T_3 = 2$ and $T_{n+3} = T_{n+2} + T_{n+1} + T_n$ for all $n \geq 1$.

Theorem 5 (F. Luca, A. Montejano, L. Szalay and A. Togbé, 2017.) *Let* (X_n, Y_n) *be the nth solution of the Diophantine equation*

$$X^2 - dY^2 = \pm 1. \tag{4}$$

The equation $X_n = T_m$ *has at most one solution* (n, m) *except:*

(i) $(n, m) = (1, 3)$ *and* $(2, 5)$ *in the* $+$ *case* $(d = 3)$*;*

(ii) $(n, m) = (1, 1),\ (1, 2),\ (3, 5)$ *in the* $-$ *case* $(d = 2)$*.*

We next give the main idea of the proof of Theorem 2. Let

$$(\alpha, \beta) = \left(\frac{1 + \sqrt{5}}{2}, \frac{1 - \sqrt{5}}{2} \right), \quad \delta = X_1 + \sqrt{d} Y_1.$$

Then the equation $F_n = X_m$ is equivalent to

$$\frac{\alpha^n - \beta^n}{\sqrt{5}} = \frac{\delta^m + \delta^{-m}}{2}, \text{ in integers } n \geq 1, m \geq 1.$$

This implies

$$n \log \alpha + \log(2/\sqrt{5}) - m \log \delta = O\left(\min\left\{ \frac{1}{\alpha^n}, \frac{1}{\delta^m} \right\} \right).$$

Linear forms in logs give $m \ll \log n$ and $n \ll \log \delta \log n$. Unfortunately we don't know δ. But say we have another such relation $F_{n'} = X_{m'}$. Then also

$$n' \log \alpha + \log(2/\sqrt{5}) - m' \log \delta = O\left(\min\left\{\frac{1}{\alpha^{n'}}, \frac{1}{\delta^{m'}}\right\}\right).$$

Then we do some linear algebra and assuming $n < n'$, we get

$$(n'm - m'n) \log \alpha - (m - m') \log(2/\sqrt{5}) = O\left(\frac{n'}{\alpha^n}\right).$$

This gives $n \ll \log n'$. Since $n \gg \log \delta$, we get that $\log \delta \ll \log n'$. Thus, $n' \ll (\log \delta) \log n' \ll (\log n')^2$, so everything is bounded. This idea ended up being very fruitful.

Let $2\mathcal{F} = \mathcal{F} + \mathcal{F}$ be the set of numbers which can be written as a sum of two Fibonacci numbers.

Theorem 6 (C. A. Gómez and F. Luca, L., 2018.) *Let (X_n, Y_n) be the nth solution of the Diophantine equation*

$$X^2 - dY^2 = \pm 1. \tag{5}$$

The equation $X_n \in 2\mathcal{F}$ has at most one solution n except for $d \in \{2, 3, 5, 11, 30\}$.

Is it true that for every $k \geq 3$ there are only finitely many d such that $X_n \in k\mathcal{F}$ has more than one solution n? Here

$$k\mathcal{F} = \mathcal{F} + \mathcal{F} + \cdots + \mathcal{F}.$$

We have no idea, If we replace $k\mathcal{F}$ by the set of positive integers having at most k ones in their binary expansion, then there are infinite many d such that X_n has at most two ones in it's binary expansion for both $n = 1, 2$. Suppose that $\mathcal{F}^2 = \mathcal{F} \cdot \mathcal{F}$ is the sequence of numbers which are products of two Fibonacci numbers.

Theorem 7 (F. Luca, A. Montejano, L. Szalay and A. Togbé, 2017.) *Let (X_n, Y_n) be the nth solution of the Diophantine equation*

$$X^2 - dY^2 = \pm 1. \tag{6}$$

The equation $X_n \in \mathcal{F}^2$ has at most one solution n except for $d \in \{2, 3, 5\}$.

Now, we move on to generalized k-Fibonacci numbers. For an integer $k \geq 2$ consider the following generalization of the Fibonacci sequence $\mathcal{F}^{(k)} = \{F_n^{(k)}\}_{n \geq -(k-2)}$ given by

$$F_n = F_{n-1} + \cdots + F_{n-k} \qquad n \geq 2,$$

where $F_{2-k} = F_{3-k} = \cdots = F_0 = 0$, $F_1 = 1$. When $k = 2$, 3 one obtains the Fibonacci and Tribonacci sequences, respectively.

Theorem 8 (M. Ddamulira and F. Luca, 2019.) *Let $k \geq 4$ be a fixed integer. Let $d \geq 2$ be a square-free integer. Assume that*

$$X_{n_1} = F_{m_1}^{(k)}, \qquad \text{and} \quad X_{n_2} = F_{m_2}^{(k)} \tag{7}$$

for positive integers $m_2 > m_1 \geq 2$ and $n_2 > n_1 \geq 1$, where X_n is the x–coordinate of the nth solution of the Pell equation

$$X^2 - dY^2 = \pm 1.$$

Put $\epsilon = X_1^2 - dY_1^2$. Then, either:

(i) $n_1 = 1$, $n_2 = 2$, $m_1 = (k+3)/2$, $m_2 = k+2$ *and* $\epsilon = 1$*; or*

(ii) $n_1 = 1$, $n_2 = 3$, $k = 3 \times 2^{a+1} + 3a - 5$, $m_1 = 3 \times 2^a + a - 1$, $m_2 = 9 \times 2^a + 3a - 5$ *for some positive integer a and* $\epsilon = 1$.

For more explanations of the exceptions we have:
For $k \geq 2$ one has

$$\begin{aligned} F_n^{(k)} &= 2^{n-2} && \text{for} \quad n \in [2, k+1]; \\ F_n^{(k)} &= 2^{n-2} - (n-k)2^{n-k-3} && \text{for} \quad n \in [k+2, 2k+1]. \end{aligned}$$

For suitable n and k it might happen that

$$F_n^{(k)} \quad = \quad 2^{n-2} - (n-k)2^{n-k-3} = 2x^2 - 1,\ 4x^3 - 3x$$

for some positive integer x which is necessarily a power of 2. Such equations give solutions to $F_{n_1}^{(k)} = X_1$ and $F_{n_2}^{(k)} = X_2$ or X_3, respectively. Next, let $\mathcal{F}act = \{m! : m \geq 1\}$.

Theorem 9 (S. Laishram, F. Luca and M. Sias, 2019.) *Let (X_n, Y_n) be the nth solution of the Diophantine equation*

$$X^2 - dY^2 = \pm 1. \tag{8}$$

The equation $X_n \in \mathcal{F}act$ implies $n = 1$.

To prove Theorem 9, we take a round about way and look at members of Lucas sequences which are products of factorials. Let r, s be coprime integers, $r^2 + 4s \neq 0$. Let α, β with $|\alpha| \geq |\beta|$ be the roots of

$$x^2 - rx - s = 0.$$

Assume $(r, s) \neq (1, -1),\ (-1, -1)$. The Lucas sequence of the first kind and second kind $\{U_n\}_{n\geq 0}$, and $\{V_n\}_{n\geq 0}$ of parameters (r, s), respectively, have its general terms given by

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \quad V_n = \alpha^n + \beta^n \quad \text{for all} \quad n \geq 0.$$

Alternatively, one can define them by setting $U_0 = 0,\ U_1 = 1,\ V_0 = 2,\ V_1 = r$ and imposing that the recurrence

$$W_{n+2} = rW_{n+1} + sW_n \qquad \text{holds for all} \qquad n \geq 0$$

is satisfied for both $\{W_n\}_{n\geq 0} \in \{\{U_n\}_{n\geq 0}, \{V_n\}_{n\geq 0}\}$. When $r = s = 1, U_n = F_n$ the sequence of Fibonacci numbers.

Theorem 10 (F. Luca and P. Stanica, 2006.) *The largest solution of the equation*

$$F_{n_1}F_{n_2}\cdots F_{n_t} = m_1!\cdots m_k!$$

in integers $1 \le n_1 < \cdots < n_t$ *and* $1 \le m_1 \le m_2 \le \cdots \le m_k$ *is*

$$F_1F_2F_3F_4F_5F_6F_8F_{10}F_{12} = 11!$$

Letting

$$\mathcal{P}F = \{\prod_{i=1}^{k} m_i! : k \ge 0,\ m_i \ge 1\}$$

be the set of positive integers which are products of factorials, one can prove easily that if $\{U_n\}_{n\ge 0}$ is a Lucas sequence, then

$$|U_n| \in \mathcal{P}F \tag{9}$$

has only finitely many solutions n. In fact, let us prove it. Write

$$|U_n| = m_1!\cdots m_k!, \qquad 1 \le m_1 \le m_2 \le \cdots \le m_k.$$

The left–hand side is $\le 2|\alpha|^n$. For $n \ge 31$, the left–hand side has, by the Primitive Divisor Theorem, proved by Bilu, Hanrot, Voutier in 2001, a prime factor $p \ge n-1$, which must divide $m_k!$. Thus, $m_k \ge n-1$, so $m_k! \ge 2((n-1)/e)^{n-1}$. Hence, we got

$$2|\alpha|^n \ge 2((n-1)/e)^{n-1},$$

so $n = O(|\alpha|)$.

We would like to have an absolute bounded on n which does not depend on α. This is contest of the next theorem.

Theorem 11 (S. Laishram, F. Luca and M. Sias, 2019.) *In equation* (9)*, we have:*

(i) $n \le 3 \times 10^5$.

(ii) If additionally, the roots α, β are real, then $n \leq 210$.

(iii) Further, if $s = \pm 1$, then $n \leq 150$.

The same bounds hold if we replace U_n by V_n in (9).

The general idea is to study on one hand the size of the two sides of (9) and on the other hand the arithmetic information obtained from considering the multiplicative contribution to the sides of (9) of the *p*rimitive prime factors of U_n. The size argument part is easy. On the one–hand,

$$\log |U_n| \leq \log 2 + n \log |\alpha|.$$

On the other hand

$$\log \left(\prod_{i=1}^{k} m_i! \right) \geq \log 2 + \sum_{i=1}^{k} (m_i - 1)(\log m_i - 1).$$

So,

$$n \log |\alpha| \geq \sum_{i=1}^{k} (m_i - 1)(\log m_i - 1). \tag{10}$$

Now for the primitive prime factors. These are the primes $p \mid U_n$ and $p \nmid U_m$ for any $1 \leq m < n$. Also, as a technical condition, we assume that $p \nmid |\Delta|$. It is known that in the left,

$$\sum_{\substack{p^\alpha \| U_n \\ p \text{ primitive}}} \log p^\alpha \geq \log \left(\frac{|\Phi_n(\alpha, \beta)|}{n} \right).$$

Here

$$\Phi_n(x, y) = \prod_{\substack{1 \leq k \leq n \\ (k,n)=1}} \left(x - \exp(\frac{2\pi i k}{n} y) \right)$$

is the homogenization of the n^{th} cyclotomic polynomial. The left–hand side can be lower bounded as

$$\log \left(\frac{|\Phi_n(\alpha, \beta)|}{n} \right) \geq (\phi(n) - 1) \log |\alpha| - C_1 2^{\omega(n)} (\log n)^2 \log |\alpha| \tag{11}$$

with some explicit constant C_1. In the right–hand side, these primes are at most the primes $p \equiv \pm 1 \pmod{n}$, which divide $m_1!m_2! \cdots m_k!$. Using the known formula for the contribution of a prime in a factorial, we get that in the right this is at most

$$\leq \sum_{m_i \geq n-1} (m_i - 1) \sum_{\substack{p \equiv \pm 1 \pmod{n} \\ p \leq m_i}} \frac{\log p}{p-1}.$$

Using the Montgomery–Vaughan bound

$$\pi(x; b, a) \leq \frac{2x}{\phi(b) \log(x/b)} \qquad \text{valid for all} \qquad x \geq b,$$

for the number of primes $p \equiv a \pmod{b}$ with $p \leq x$ and Abel summation formula, we get the following upper bound on the right–hand side

$$\left(\frac{4(1 + \log\log n}{\phi(n)}\right) \sum_{m_i \geq n-1} (m_i - 1)(\log m_i - 1),$$

which combined with (10) gives an upper bound of

$$\left(\frac{4(1 + \log\log n}{\phi(n)}\right) n \log|\alpha|$$

on the contribution of the primitive primes from the right–hand side. Comparing the last bound with (11), we get

$$(\phi(n)-1)\log|\alpha| - C_1 2^{\omega(n)} \log|\alpha| (\log n)^2 < \left(\frac{4(1 + \log\log n)}{\phi(n)}\right) n \log|\alpha|.$$

A paper of Voutier shows that one can take $C_1 = 73$. This gives $n < 18 \times 10^6$. Then one goes down easily to about 2×10^6. For $n \leq 3 \times 10^5$ more ingredients are needed.

What does this have to do with X-coordinates of Pell equations and factorials?

Well say, $X_k = n!$. Then

$$X_k = \frac{1}{2}(\alpha^k + \beta^k), \quad \alpha = X_1 + d\sqrt{Y_1} = X_1 + \sqrt{X_1^2 - \varepsilon}, \quad \varepsilon \in \{\pm 1\},$$

and β is the conjugate of α. So, we get

$$\alpha^k + \beta^k = V_k = 2!n!,$$

therefore by the previous results, $k < 150$. One may assume that k is prime. If $k = 2$, then $X_2 = 2X_1^2 \pm 1$ is odd and > 1, so it is not a product a product of factorials. Say $k = p$ and $p \in [3, 150]$ is a prime. Then $X_p = P_p(X_1)$ is a polynomial of degree p in X_1. Take $p = 3$, $\varepsilon = 1$. Then we need to solve

$$X_3 = X_1(4X_1^2 - 3) = n!$$

In the left, the only factors that divide $4X_1^2 - 3$ are (aside possibly from 3 to exponent exactly 1), only primes q such that $(3/q) = 1$. These occupy two of the four possible progressions modulo 12 which may contain infinitely many primes, so half of all the primes, and they contribute the factor $4X_1^2 - 3$ of X_3 so multiplicatively about

$$X_3^{2/3}.$$

In the right, these primes, by the equidistribution of the primes in progressions modulo 12, will contribute about

$$n!^{1/2} = X_3^{1/2}.$$

We get a contradiction for large X_3. To quantify what large means we need explicit estimates for primes in progressions with ratio 12. More generally, we need for all other all primes $p \in [5, 150]$ explicit estimates for the number of primes $q \leq x$ which are in a certain progression modulo p. We used the following result.

Theorem 12 (Bennett, Martin, Bryant and Rechnitzer, 2018.) *Let $m \leq 1200$, $\gcd(a, m) = 1$. For all $x \geq 50m^2$ we have*

$$\frac{x}{\phi(m)\log x} < \pi(x; m, a) < \frac{x}{\phi(m)\log x}\left(1 + \frac{5}{2\log x}\right).$$

Another natural question appears which is what about Y-coordinates of Pell equations in sequences? How about $Y_n \in \mathcal{U}$ for your favourite set $\mathcal{U}$? Here the problem is slightly different. There are infinitely many binary recurrences $\mathcal{U}$ such that $Y_n \in \mathcal{U}$ has two solutions n. For example, this is so if $1 \in \mathcal{U}$ and $\mathcal{U}$ contains infinitely many even numbers. It is also so for $\mathcal{U} = \{2^m - 1 : m \geq 1\}$ since taking $d = 2^{2a} - 1$ for some a, then both $Y_1 = 1$ and $Y_3 = 2^{2a+2} - 1$ are in $\mathcal{U}$. However, this is best possible:

Theorem 13 (B. Faye and F. Luca, 2016.) *If $\mathcal{U} = \{U_m\}_{m \geq 1}$ is a binary recurrent sequence of integers, then $Y_n = U_m$ has at most two solutions (n, m) provided $d > d_0(\mathcal{U})$, where $d_0(\mathcal{U})$ is effectively computable.*

In case $\mathcal{U} = \{2^m - 1 : m \geq 1\}$, one can take $d_0(\mathcal{U}) = 1$.

References

[1] A. Dossavi-Yovo, F. Luca and A. Togbé, *On the x-coordinate of Pell equations which are rep-digits*, Publ. Math. Debrecen **88** (2016), 381-399.

[2] F. Luca and A. Togbé, *On the x-coordinates of Pell equations which are Fibonacci numbers*, Mathematica Scandinavica **122** (2018), 18-30.

[3] B. Faye and F. Luca, *On X-Coordinates of Pell Equations that Are Repdigits*, Fibonacci Quart. **56** (2016), 52-62.

[4] B. Kafle, F. Luca and A. Togbé, *x-coordinate of Pell equations which are Fibonacci numbers II*, Periodica Mathematica Hungarica (2018), 1-11.

[5] F. Luca, A. Montejano, L. Szalay and A. Togbé, *On the x-coordinate of Pell equations which are Tribonacci numbers*, Acta Arithmetica **179** (2017), 25-35.

[6] C. A. Gomez and F. Luca, *Zeckendorf representations with at most two terms to x-coordinates of Pell equations*, Science China Mathematics (2018), 1-16.

[7] M. Ddamulira and F. Luca, *On the x-coordinates of Pell equations which are k-generalized Fibonacci numbers*, J. of Number Theory, to appear (2019).

[8] S. Laishram, F. Luca and M. Sias, *On members of Lucas sequences which are products of factorials*, preprint (2019).

[9] F. Luca and P. Stanica, $F_1\ F_2\ F_3\ F_4\ F_5\ F_6\ F_7\ F_8\ F_9$=*11!*, Portugaliae Mathematica **63** (2006), 251-260.

[10] Y. Bilu , G. Hanrot , P. M. Voutier, *Existence of primitive divisors of Lucas and Lehmer numbers*, J. Reine Angew. Math **539** (2001), 75-122.

[11] H. L. Montgomery and R. C. Vaughan, *Exponential sums with multiplicative coefficients*, Invent. Math. **43** (1977), 69âĂŞ82.

[12] P. M. Voutier, *Primitive divisors of Lucas and Lehmer sequences, III*, Math. Proc. Cambridge Philos. Soc. **123** (1998), 407-419.

[13] M. A. Bennett, G. Martin, K. Bryant and A. Rechnitzer, *Explicit bounds for primes in arithmetic progressions*, Illinois Journal of Mathematics **62** (2018), 427-532.

Andam Mustafa
Mathematics and Physics Dep.
Roma Tre University
Largo San Leonardo Murialdo,1 .
email: andam.mustafa@uniroma3.it

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 5, *Number* 1, *March* 2020, *pages* 81-87

Sara Checcoli

Fields of algebraic numbers with bounded local degrees and their Galois groups

Written by Lorenzo Pagani

1 Uniformly bounded local degrees

A field $L \subset \overline{\mathbb{Q}}$ *has bounded local degree at a prime number* p if for every valuation v of L extending the p-adic one there exists a constant d_p such that $[L_v : \mathbb{Q}_p] \leq d_p$. We say that L *has uniformly bounded local degrees* if the constants d_p's can be chosen independently on p.

Numbers fields are the first examples of fields with uniformly bounded local degrees. More interesting examples are given by some infinite extensions, namely the compositum of all the extensions of degree at most d of a number field. These extensions have uniformly bounded local degrees as shown in [4] by Bombieri and Zannier.

Furthermore if we assume the extension L to be Galois over a number field, we can completely characterize the property of having uniformly bounded local degrees with properties on the Galois group.

Theorem 1 *Let K be a number field and L be a Galois extension of K. Then L has uniformly bounded local degrees if and only if the group $Gal(L/K)$ has finite exponent.*

One implication is proved in [7], while the full statement is in [5].

We are interested in the following problem:

Question 1 *Let L be a Galois extension of a number field K with Galois group G. Is there a group theoretical property on G equivalent to the boundedness of local degrees of L at some given primes?*

2 Bogomolov property

The question about boundedness of local degrees is interesting also in connection with the Bogomolov property, that we will recall in this section.

We denote by $h : \overline{\mathbb{Q}} \to \mathbb{R}_{\geq 0}$ the absolute logarithmic Weil height. A field $L \subset \overline{\mathbb{Q}}$ *has the Bogomolov property if there exists a constant* $C > 0$ *such that for every* $\alpha \in L$ *which is not* 0 *nor a root of unity, then* $h(\alpha) \geq C$.

Examples of fields with Bogomolov property are number fields as a consequence of Northcott's theorem. However, deciding whether a given infinite extension of $\mathbb{Q}$ has the Bogomolov property is generally a difficult task. Some examples of fields with the above property are:

1. abelian extensions of a number field by the results of Amoroso and Dvornicich when the base field is $\mathbb{Q}$ in [1], and by Amoroso and Zannier for any number field in [2].

2. The field of totally real numbers, proved by Schinzel in [11].

3. The Galois extension of $\mathbb{Q}$ with bounded local degrees at some prime. This result is due to Bombieri and Zannier in [4] and can be seen as the p-adic analogue of Schinzel's result mentioned above.

In [3] Theorem 1.2 states, in particular, that the Bogomolov property holds for any Galois extension L of a number field K having Galois

group G and such that $L^{Z(G)}$ has bounded local degrees at some primes, where $L^{Z(G)}$ denotes the subfield of L fixed by the center $Z(G)$ of G.

Following [3], the Bogomolov property can be defined also for groups: a profinite group *G has the Bogomolov property if, for every number field K and for every Galois extension L of K, with Galois group isomorphic to G, the field L has the Bogomolov property*.

Let G be a profinite group such that for every number field K and for every extension L of K with Galois group isomorphic to G the extension $L^{Z(G)}$ has bounded degrees at some given primes, then by the above mentioned results G has the Bogomolov property. In particular if $G/Z(G)$ has finite exponent, hence $L^{Z(G)}$ has uniformly bounded local degrees, then G has the Bogomolov property; this case include G finite or abelian.

A natural and still open question is the following:

Question 2 *Are we able to characterize group G such that every realization of G as a Galois group over a number field has bounded local degree at some primes? More generally, can we found new groups with the Bogomolov property?*

Before going further, we remark that, as shown by Amoroso, David and Zannier in [3], there are groups without the Bogomolov property. Let $\mathbb{Q}^{\mathrm{tr}}$ be the field of totally real number, as shown in [11] it has the Bogomolov property. However the Galois group G of $\mathbb{Q}^{\mathrm{tr}}/\mathbb{Q}$ has not the Bogomolov property. Indeed, let i be a solution of $X^2 + 1 = 0$, the group G can be realized as the Galois group of the extension $\mathbb{Q}^{\mathrm{tr}}(i)$ over $\mathbb{Q}(i)$. Here we consider the sequence

$$\alpha_n = \left(\frac{2-i}{2+i}\right)^{1/n}$$

and we get that $h(\alpha_n) \to 0$. We observe that the elements α_n have absolute value 1 for every archimedean places: this fact suffices to show that they lies in $\mathbb{Q}^{\mathrm{tr}}(i)$.

3 Bounded local degrees at some primes

In this section we give an answer to our first question; namely if, for a Galois extension of a number field, the property of having bounded local degrees at some prime can be completely characterized via theoretical properties of the Galois group. The answer is negative as the following result shows.

Theorem 2 *Let $\mathcal{S}$ be a set of rationals primes and let K be a number field. There exist groups G each admitting two realizations over K: one with bounded local degrees at all primes in $\mathcal{S}$ and the other with unbounded local degrees at all primes in $\mathcal{S}$.*

We recommend to look at [6] to get a more precise statement about the properties that these groups G need to have. In particular the groups used in the proof are infinite direct products of certain finite groups G_m's; clearly these products need to have unbounded exponent.

The key properties of the groups considered is that they guarantee the existence of solutions of some specific Grunwald problems. To be more precise let $G = \prod_{m\in\mathbb{Z}_{>0}} G_m$ and $\mathcal{S} = \{p_1, p_2, p_3, \dots\}$, we define $\mathcal{T}_m$ the set of primes of K lying over $\{p_1, \dots, p_m\}$. Then, by the choice of the G_m's, for every family of cyclic groups $\left\{G_{m,v} \leq G_m\right\}_{v\in\mathcal{T}_m}$ there exists a field extension L_m over K such that:

1. the field L_m is Galois over K with group G_m,
2. for every $v \in \mathcal{T}_m$ the extension L_m has local Galois group at v given by $G_{m,v} \leq G_m$.

Moreover the fields L_m's can be chosen to be linearly disjoints. This can be achieved for example by taking the groups G_m's with coprime orders.

The above groups G_m's exist, thanks to the work of many authors on the Grunwald problem. Examples of them are the followings:

1. abelian groups of odd order, due to results of Grunwald in [9] and Wang in [12].

2. Solvable groups of order prime to the number of roots of unity of K, proven by Neukirch in [10].

3. Iterated semidirect products of abelian groups of order not divisible by the primes in $\mathcal{S}$, by the result of Demarche, Lucchini-Arteche and Neftin in [8].

Realization with bounded local degrees

We choose $G_{m,v}$ to be trivial. Hence we get an extensions L_1 with trivial degrees at primes dividing p_1, an extension L_2 with trivial degrees at primes dividing p_1p_2, and so on. Taking the compositum of all the L_m's, since they are disjoint, we can control the local degree at a prime dividing p_i with

$$[K : \mathbb{Q}] \prod_{j=1}^{i-1} |G_m|$$

and so it has bounded local degrees at the primes in $\mathcal{S}$.

Realization with unbounded local degrees

Since the exponent of G is not finite, there exists a sequence of indexes $\mathcal{M} = \{m_n\}_{n\in\mathbb{Z}_{>0}}$ such that $m_n < m_{n+1}$ and the group G_{m_n} have an element of order n. Now if $m = m_n \in \mathcal{M}$ we choose $G_{m_n,v}$ to be a cyclic group of order n for every $v \in \mathcal{T}_{m_n}$; if $m \notin \mathcal{M}$ we set $G_{m,v} = 1$. Then proceeding as in the case of bounded local degrees we get linearly disjoint extensions L_m's such that their compositum has unbounded local degrees at the prime in $\mathcal{S}$, since if $m_n \in \mathcal{M}$ then the extension L_{m_n} has local degrees n for every prime in $\mathcal{T}_{m_n}$.

We finally observe that the Theorem above does not give us new examples of group with Bogomolov property and that we still don't know if there exists a property on group that implies the boundedness of the local degrees at some given prime. However, the result above seems to suggest the fact that if such a property exists, a group that satisfies it should not be a direct product.

References

[1] F. Amoroso and R. Dvornicich, *A lower bound for the height in abelian extensions*. Journal of Number Theory **80** (2000), 260-272.

[2] F. Amoroso and U. Zannier, *A uniform relative Dobrowolski's lower bound over abelian extensions*. Bull. Lond. Math. Soc. **42** no. 3 (2010), 489-498.

[3] F. Amoroso, S. David and U. Zannier, *On fields with property (B)*. Proceedings of the AMS **142** 6 (2014), 1893-1910.

[4] E. Bombieri and U. Zannier, *A note on heights in certain infinite extensions of* $\mathbb{Q}$. Rend. Mat. Acc. Lincei **12** (2001), 5-14.

[5] S. Checcoli, *Fields of algebraic numbers with bounded local degree and their properties*. Trans. Amer. Math. Soc. **365** no. 4 (2013), 2223-2240.

[6] S. Checcoli, *A note on Galois groups and local degrees*. Manuscripta Mathematica **159**, Issue 1-2, (2019) 1-12.

[7] S. Checcoli and U. Zannier, *On fields of algebraic numbers with bounded local degrees.* C. R. Acad. Sci. Paris **349** no. 1-2 (2011), 11-14.

[8] C. Demarche, G. Lucchini Arteche and D. Neftin, *The Grunwald problem and approximation properties for homogeneus spaces*. Annales de l'institut Fourier, **63** no. 3 (2017), 1009-1033.

[9] W. Grunwald, *Ein allgemeines Existenztheorem für algebraische Zahlkörper*. J. Reine Angew. Math. **169** (1933), 103-107.

[10] J. Neukirch, *On solvable number fields*. Invent. Math. **53** (1979), 135-164.

[11] A. Schinzel, *On the product of conjugates outside the unit circle of an algebraic number*. Acta Arith. **24** (1973), 385-399.

[12] S. Wang, *On Grunwald's theorem*. Ann. of Math. **51** (1950), 471-484.

Lorenzo Pagani
Departement of Mathematics
Universitá di Roma "La Sapienza"
Piazzale Aldo Moro 5
00185 Roma Italy.
email: pagani@mat.uniroma1.it

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 5, *Number* 1, *March* 2020, *pages* 89-98

Marusia Rebolledo

Abelian varieties with large Galois image

Written by Mohamadou Sall

1 Representations associated to abelian varieties

In this talk, we will consider mod ℓ Galois representations attached to abelian varieties over number fields, especially over $\mathbb{Q}$.

Let A be an abelian variety of dimension g over a number field K. Let $\ell \geq 2$ be a prime number and $A[\ell]$ the subgroup of $\ell-$torsion points of A. Then the natural action of the absolute Galois group $\mathbf{G}_K = Gal(\bar{K}/K)$ on the set of $\ell-$torsion points $A[\ell]$ of A gives rise to a continuous representation

$$\rho_{A,\ell} : Gal(\bar{K}/K) \longrightarrow Aut(A[\ell]).$$

After a choice of basis of $A[\ell]$ as a $2g-$dimensional $\mathbf{F}_\ell-$ vector space, we get an isomorphism $GL_{2g}(A[\ell]) \cong GL_{2g}(\mathbf{F}_\ell)$, and will still denote by $\rho_{A,\ell}$ the induced representation $Gal(\bar{K}/K) \longrightarrow GL_{2g}(\mathbf{F}_\ell)$. The question we will be interested in is "how large can be its image?". We won't consider here the $\ell-$adic and the adelic representations.

Remark 1 *The initial motivation of such question is the Galois inverse problem. It concerns whether or not every finite group appears as the Galois group of some Galois extension of the rational numbers* $\mathbb{Q}$.

2 Open image theorems

The starting point of a lot of questions given below is the following famous *Serre's open image theorem*. This theorem, formulated on mod ℓ representation, ensures that for A a non CM elliptic curve, i.e, such that $End_{\bar{K}}(A) = \mathbb{Z}$ over a number field K, and for ℓ great enough, the image of the mod ℓ representation is as large as possible. The properties of $\rho_{A,\ell}$ are well understood if A is an elliptic curve with complex multiplication (CM), i.e, $End_{\bar{K}}(A) \neq \mathbb{Z}$ (see [3], section 4.5). It depends on the decomposition of ℓ in the field of complex multiplication.

Theorem 1 (Serre - 1972) *Let A/K be a non CM elliptic curve. Then there exists $B_{A,K} > 0$ such that for all $\ell > B_{A,K}$, $\rho_{A,\ell}(\mathbf{G}_K) = GL_2(\mathbf{F}_\ell)$.*

A natural question that arises is: does this result generalize to the case of dimension $g > 1$?

First, notice that structures on A (coming from endomorphism, polarization, ...) impose some constraints on the image, $Im(\rho)$, of ρ. For instance if A is principally polarized, which means that there is an isomorphism between A and its dual $\check{A}$, given by an ample divisor, then the Weil pairing induces a pairing on $A[\ell] \times A[\ell]$

$$\langle , \rangle : A[\ell] \times A[\ell] \longrightarrow \mu_\ell(\bar{K})$$

which is G_K-equivariant so such that for all $P, Q \in A[\ell]$

$$\langle P^\sigma, Q^\sigma \rangle = \langle P, Q \rangle^\sigma.$$

As a consequence the image of $\rho_{A,\ell}$ lies inside the general symplectic group $GSp(A[\ell], \langle , \rangle)$ of $A[\ell]$ for this pairing [1] . After a good choice of basis $GSp(A[\ell], \langle , \rangle)$ is isomorphic to $GSp_{2g}(\mathbf{F}_\ell)$. Let recall briefly that, the general symplectic group over $\mathbf{F}_\ell$ of order $2g$ is the linear group

$$GSp_{2g}(\mathbf{F}_\ell) = \{M \ : \ \exists\, a \in \mathbf{F}_\ell^*, \ {}^tMJM = aJ\}$$

where J is the matrix

$$\begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix}.$$

Remark 2 *In particular* $GSp_2(\mathbf{F}_\ell) = GL_2(\mathbf{F}_\ell)$.

Serre proved the following partial generalization of Theorem 1 to the case $g > 1$:

Theorem 2 (Serre) *Let A/K be a principally polarized abelian variety of dimension $g = 2$ or 6 or odd such that $End(A) = \mathbb{Z}$. Then there exists $B_{A,K} > 0$ such that for $\ell > B_{A,K}$, $\rho_{A,\ell}(\mathbf{G}_K) = GSp_{2g}(\mathbf{F}_\ell)$.*

This result is not true for any dimension g as shows a famous counterexample of Mumford [7], for $g = 4$.

3 Some questions

A series of questions arises from Serre's above theorem. In what follows A will denote a principally polarized abelian variety of dimension g over a number field K, and $End(A) = \mathbb{Z}$, ℓ a prime number, and $B_{A,K}$ a constant.

1. For a given A, can we determine an explicit bound $B_{A,K}$?

[1] Let R be a commutative ring, M a finitely generated $R-$module, equipped with a non-degenerate alternating bilinear form $\langle \ , \ \rangle$. Then $GSp(M, \langle \ , \ \rangle)$ is the group of $\varphi \in Aut_R(M)$ such that for some $a \in R^\times$, $\langle \varphi v, \varphi w \ \rangle = a\langle v, w \rangle$ for all $v, w \in M$.

2. or at the contrary for a given ℓ, can we give an explicit abelian variety A_ℓ, such that $\rho_{A_\ell,\ell}(\mathbf{G}_K) = GSp_{2g}(\mathbf{F}_\ell)$? or even a whole family of such A_ℓ.

Let's even ask something stronger.

3. (Uniformity conjecture) does there exist a constant $B > 0$ such that for all prime number $\ell > B$, and all abelian variety A, $\rho_{A,\ell}(\mathbf{G}_K) = GSp_{2g}(\mathbf{F}_\ell)$?

4. Does there exist an abelian variety A, such that for all ℓ, $\rho_{A,\ell}(\mathbf{G}_K) = GSp_{2g}(\mathbf{F}_\ell)$? and if so can we determine A explicitly?

Let first examine these questions more precisely in the case $g = 1$.

Question 1 is motivated by the fact that Theorem 1 is not effective in all generality. In [3], Serre gave effective results for semi-stable elliptic curves (see [[3], 5.4 proposition 21 and corollary 1). Later on, Serre [4] gave the explicit upper bound:

$$B_{A,\mathbb{Q}} \leq c.\log(N_A)(\log\log N_A)^3$$

where N_A is the conductor of the elliptic curve, and c an absolute (and effectively computable) constant. However this bound is conditional to GRH. In [5] Masser and Wustholz give a general upper bound for $B_{A,K}$:

$$B_{A,K} \leq C \cdot max(h_A, d)^\gamma,$$

where d is the degree of the number field K, $h_A = \log(h(j(A))$, and γ and C are constants.

Over $\mathbb{Q}$, Alain Kraus [9] and then Cojocaru [8] gave another unconditional bound in terms of the conductor using the modularity of elliptic curves over $\mathbb{Q}$, namely

$$B_{A,\mathbb{Q}} \leq C \cdot N_A \cdot (\log\log N_A)^{\frac{1}{2}}.$$

Moreover in [6] David Zywina gives the first general bounds [10] of the index in terms of basic invariants of an elliptic curve A without CM. He shows that the product [2]

$$\prod_{l \text{ exceptional for } A} l \leq B_{A,\mathbb{Q}}^{b_A},$$

where b_A is the number of primes of bad reduction for A. The approach used by Zywina was also limited to $\mathbb{Q}$. Zywina also gave an explicit elliptic curve answering to question 4 (so to question 3).

The third question is an interesting and largely open question, even for non CM elliptic curves over $\mathbb{Q}$. It is known as Serre's uniformity conjecture (in the case of elliptic curves).

Note that all the preceding results deal with abelian varieties of dimension $g = 1$. In his thesis [2] Lombardo gives explicit results for question 1 for some cases of abelian varieties of dimension $g \geq 1$, like products of non-CM elliptic curves over a number field K.

In what follows, we focus on questions 2 and 4.

4 Some progress on questions 2 and 4 for $g > 1$

In the sequel we will focus on questions 2 and 4, and we set $K = \mathbb{Q}$ and $g \geq 3$. The following results are motivated and based on ideas of previous works for $g = 2$ of lot of authors, as for instance, Le Duff, Arias-de-Reyna, Vila, Dieulefait.

We start with the following theorem which concerns the Jacobian, $Jac(C)$, of genus 3 curve. It was independently proved by Zywina, and by Samuele Anni et al.

[2] A prime number ℓ is exceptional, relative to a pair (A, K), if the map $\rho_{A,\ell}$ is not surjective.

Theorem 3 (Anni-Lemos-Siksek, Zywina 2016) *There is an explicit genus* 3 *curve* $C/\mathbb{Q}$ *such that for all prime number* $\ell \geq 3$, $\rho_{Jac(C),\ell}(\mathbf{G}_{\mathbb{Q}}) = GSp_6(\mathbf{F}_\ell)$.

The curve, given by Zywina is the quartic plane curve given by the equation

$$x^3y - x^2y^2 + x^2z^2 + xy^3 - xyz^2 - xz^3 - y^4 + y^3z - y^2z^2 - yz^3 = 0,$$

and the curve given by Anni, Lemos, and Siksek is an hyperelliptic curve

$$C : y^2 + (x^4 + x^3 + x + 1)y = x^6 + x^5.$$

In the following theorem, Arias de Reyna et al. gave another answer to question 2: for a given prime number ℓ, it gives an infinite family of abelian varieties answering to the question.

Theorem 4 ([1]) *Let* $\ell \geq 13$ *be a prime number. For all primes* $p \neq q$ *such that* $p \neq \ell, q > 1.82\ell^2$, *there exists* $f_p, f_q \in \mathbb{Z}[x, y]$ *of* same type, *such that for all* $f \in \mathbb{Z}[x, y]$ *of same type, if*

$$f \equiv f_q \pmod{q} \text{ and } f \equiv f_p \pmod{p^3} \tag{1}$$

then f *defines a genus* 3 *curve* C *such that* $\rho_{Jac(C),\ell}(\mathbf{G}_{\mathbb{Q}}) = GSp_6(\mathbf{F}_\ell)$.

Here we say that a polynomial $f(x, y)$ is of 3−hyperelliptic type if it is of the form $f(x, y) = y^2 - g(x)$, where $g(x)$ is a polynomial of degree 7 or 8 and $f(x, y)$ is of quartic type if it is homogeneous of total degree 4. Two polynomials are of the same type if both of them are either of 3−hyperelliptic type or of quartic type. In Theorem 4, f_p is explicit and f_q is algorithmically computable for a given ℓ.

Finally the following is the first result which answers to question 4 for an infinite number of g. This result is related to the double Goldbach conjecture proved by Montgomery.

Theorem 5 (Anni-Dokchitser, 2017) *Let g be an integer such that $2g+2$ satisfies the double Goldbach conjecture. Then there exist an explicit $N \in \mathbb{Z}$ and an explicit $h_0 \in \mathbb{Z}$ monic of degree $2g+2$ such that if*

1. $h \equiv h_0 \pmod{N}$,
2. *for all $p \nmid N$, $h \pmod{p}$ has no roots of multiple > 2.*

then $y^2 - h(x)$ defines a hyperelliptic curve C such that for all $\ell \geq 3$, $\rho_{Jac(C),\ell}(\mathbf{G}_{\mathbb{Q}}) = GSp_{2g}(\mathbf{F}_\ell)$.

An integer n satisfies the double Goldbach conjecture if $n = q_1 + q_2 = q_4 + q_5$ distinct pairs of primes and none of them being the largest prime $\leq n$. Note that the hypothesis is not true for $g = 1, 2, 3, 4, 5, 7$, and 13.

5 Common ideas

In this last paragraph, we will give some ideas common to the articles establishing the above results. It is now a classical strategy to use the following proposition to force the image to be large.

Proposition 1 *The following two conditions imply that $\rho_{A,\ell}(\mathbf{G}_K) = GSp_{2g}(\mathbf{F}_\ell)$.*

1. *There exist a transvection in $\rho_{A,\ell}$.*
2. *There exist F in $Im(\rho_{A,\ell})$ a non zero trace, irreducible $\pmod{\ell}$.*

The above proposition is due to a partial classification of subgroups of $GSp_{2g}(\mathbf{F}_l)$ and the fact that

$$m : GSp_{2g}(\mathbf{F}_l) \longrightarrow \mathbf{F}_l^*$$

restricted to $\rho_{A,l}$ is surjective.

In the following proposition Hall gives conditions which ensure the existence of a transvection (condition 1).

Proposition 2 *If A has potentially semistable reduction of toric dimension* 1 *above a prime number p (TR1), then for all* $\ell \nmid 6p|\phi|$, $\rho_{A,\ell}(I_{\mathfrak{p}})$ *is cyclic generated by a transvection.*

The condition (TR1) means that there is a finite extension L/K so that the special fiber at p of the Néron model of A/L over the ring of integers O_L lies in an extension

$$1 \to G_m^1 \to \mathcal{A}_{k_{\mathfrak{p}}} \to \mathcal{B} \to 1$$

where $\mathcal{B}$ is an abelian variety. We denote by $\phi = \mathcal{A}_{\overline{\mathbf{F}}_p}/\mathcal{A}^0_{\overline{\mathbf{F}}_p}$ the component group of $\mathcal{A}_{\overline{\mathbf{F}}_p}$, and $I_{\mathfrak{p}}$ is the inertia group at a prime $\mathfrak{p}$.

The above result allows Hall to establish the following.

Theorem 6 (Hall) *Let* A/K *be a principally polarized abelian variety of dimension g, with* $End(A) = \mathbb{Z}$, *and satisfying (TR1). Then there exists* $B_{A,K} > 0$ *such that for all* $\ell > B_{A,K}$, $\rho_{A,\ell}(\mathbf{G}_K) = GSp_{2g}(\mathbf{F}_\ell)$.

It is possible to prescribe (TR1) for $Jac(C)$ at p by controlling the reduction of C above p. This is the strategy adopted by [1] and Anni-Dokchitser. The ideas differ about condition 2.

In [1], Arias de Reyna et al. use a second auxiliary prime q to prescribe condition 2. By Chebotarev's theorem, it is natural to look for elements F of condition 2 as images by ρ of Frobenius elements $Frob_q$. The relation with Frobenius endomorphisms of abelian varieties is given by Honda-Tate theory. More precisely, Arias et al. show that for $\ell \geq 13$ and $q > 1.82\ell^2$ there exists an ordinary Weil$-q-$polynomial wich has non zero trace and is irreducible modulo ℓ. By Honda-Tate theory, such a Weil polynomial defines an isogeny class of simple ordinary abelian varieties of dimension 3. By results of Howe, Oort-Ueno and Serre, there exists a curve C_q defined over $\mathbf{F}_q$ with $Jac(C_q)$ in

this isogeny class. This ensures that Condition 2 holds for every curve reducing to C_q.

This method allows to obtain many distinct realisations of $GSp_6(\mathbf{F}_\ell)$ as a Galois group over $\mathbb{Q}$. However it is limited because Oort-Ueno is specific to $g = 3$, and C_q is not explicit in all generality.

References

[1] Sara Arias-de-Reyna, Cecile Armana, Valentijn Karemaker, Marusia Rebolledo, Lara Thomas and Nuria Vila, *Large Galois images for Jacobian varieties of genus 3 curves*. Acta Arith. **174(4)**, 339-366, 2016

[2] Davide Lombardo, *Représentations galoisiennes et groupe de Mumford-Tate associé á une variéte abélienne*. Théorie des nombres [math.NT]. Université Paris-Saclay, 2015.

[3] Jean-Pierre Serre, *Propriétes galoisiennes des points d'ordre fini des courbes elliptiques*. Invent. Math. 15 (1972), no. 4, 259-331.

[4] Jean-Pierre Serre, *Quelques applications du théoréme de densité de Chebotarev.* Inst. Hautes Études Sci. Publ. Math., (54):323-401, 1981.

[5] D.W. Masser and G. Wustholz, *Galois properties of division fields of elliptic curves*. Bull. London Math. Soc. 25 (1993), no. 3, 247-254.

[6] D. Zywina, *Bounds for Serre's open image theorem*. ArXiv e-prints, 1102.4656, Feb. 2011.

[7] D. Mumford, *A note of Shimura's paper "Discontinuous groups and abelian varieties"*. Math. Ann., 181:345-351, 1969.

[8] Alina Carmen Cojocaru *On the surjectivity of the Galois representations associated to non-CM elliptic curves*. Canad. Math. Bull., 48(1):16-31, 2005. With an appendix by Ernst Kani.

[9] Alain Kraus *Une remarque sur les points de torsion des courbes elliptiques*. C. R.Acad. Sci. Paris Sér. I Math., 321(9):1143-1146, 1995.

[10] Eric Larson and Dmitry Vaintrob *On the Surjectivity of Galois Representations Associated to Elliptic Curves over Number Fields* https://arxiv.org/abs/1204.0046v1

Mohamadou Sall
Department of Mathematics-Informatics
Cheikh Anta Diop University
BP 5005 DAKAR FANN, SENEGAL.
email: msallt12@gmail.com

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 5, *Number* 1, *March* 2020, *pages* 99-106

Pieter Moree

Irregular behaviour of class numbers and Euler-Kronecker constants of cyclotomic fields: the log log log devil at play

Written by Pietro Sgobba

We study two invariants for cyclotomic number fields $\mathbb{Q}(\zeta_q)$, where q is a prime, namely the first factor of the class number and the Euler-Kronecker constant. In particular, we consider the connection between a conjecture by Kummer on the asymptotic behaviour of the former and a conjecture by Ihara on the positivity of the latter.

1 The Euler-Kronecker constant

The *Euler-Mascheroni constant* γ is defined as

$$\gamma = \lim_{n\to\infty}\left(\sum_{k=1}^{n}\frac{1}{k} - \log n\right) = 0.577...$$

and in general we define the *Stieltjes constants* as

$$\gamma_r = \lim_{n\to\infty}\left(\sum_{k=1}^{n}\frac{\log^r k}{k} - \frac{\log^{r+1} n}{r+1}\right)$$

for $r \geq 0$, which arise as the coefficients of the Laurent series expansion of the Riemann zeta function:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \frac{1}{s-1} + \sum_{r=0}^{\infty} \frac{(-1)^r}{r!} \gamma_r (s-1)^r \,.$$

In particular, we have

$$\zeta(s) = \frac{1}{s-1} + \gamma + O(s-1) \,.$$

Recall that the *Dedekind-zeta function* of a number field K is defined as

$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{(N\mathfrak{a})^s} \,, \qquad \mathrm{Re}(s) > 1 \,,$$

where $\mathfrak{a}$ runs over all integral ideals of K. The Laurent series of ζ_K is such that

$$\zeta_K(s) = \frac{c_{-1}}{s-1} + c_0 + O(s-1) \,.$$

The *Euler-Kronecker constant* of K, introduced by Ihara, is then defined as $\mathcal{EK}_K := c_0/c_{-1}$, which is the constant term in the logarithmic derivative of $\zeta_K(s)$ at $s = 1$:

$$\lim_{s \to 1} \left(\frac{\zeta_K'(s)}{\zeta_K(s)} + \frac{1}{s-1} \right) = \mathcal{EK}_K \,.$$

For example, we have $\mathcal{EK}_{\mathbb{Q}} = \gamma$. The Euler-Kronecker constant satisfies

$$\mathcal{EK}_K = \lim_{x \to \infty} \left(\log x - \sum_{N\mathfrak{p} \leq x} \frac{\log N\mathfrak{p}}{N\mathfrak{p} - 1} \right) ,$$

where $\mathfrak{p}$ runs over the primes of K, so that for cyclotomic fields $\mathbb{Q}(\zeta_q)$, setting $\gamma_q := \mathcal{EK}_{\mathbb{Q}(\zeta_q)}$, the main contribution is given by the rational primes p which split completely in $\mathbb{Q}(\zeta_q)$:

$$\gamma_q = \lim_{x \to \infty} \left(\log x - (q-1) \cdot \sum_{\substack{p \leq x \\ p \equiv 1 \bmod q}} \frac{\log p}{p-1} \right) + \text{smaller order terms} \,.$$

Under the assumption of the Extended Riemann Hypothesis (ERH), Ihara, and by different methods, Ford, Luca and Moree showed the following approximation:

$$\gamma_q = \log(q^2) - q \cdot \sum_{\substack{p \le q^2 \\ p \equiv 1 \bmod q}} \frac{\log p}{p-1} + O(\log\log q)\,. \tag{1}$$

Unconditionally this estimate holds for all $C > 0$ and for all but $O(\pi(u)/(\log u)^C)$ primes $q \le u$. Assuming the Elliot-Halberstam conjecture (Conj. 1) we may replace q^2 by $q^{1+\epsilon}$ in (1).

2 Ihara's conjectures

We first introduce two standard conjectures.

Conjecture 1 (Elliot-Halberstam (EH))**.** *For every $\epsilon > 0$ and $A > 0$ we have*

$$\sum_{q \le x^{1-\epsilon}} \left|\pi(x;q,a) - \frac{\mathrm{li}(x)}{\varphi(q)}\right| \ll_{A,\epsilon} \frac{x}{\log^A x}\,,$$

where $\pi(x;q,a)$ denotes the number of primes p less than x with $p \equiv a \bmod q$, and φ is Euler's totient function.

We say that a set $\{b_1,\dots,b_k\}$ of positive integers is *admissible* if the congruence $n\prod_{i=1}^k(b_in+1) \equiv 0 \bmod p$ has $< p$ solutions for every prime p.

Conjecture 2 (Hardy-Littlewood (HL))**.** *If $\{b_1,\dots,b_k\}$ is admissible, then the number of primes $n \le x$ for which the integers b_in+1 are all prime is*

$$\gg \frac{x}{\log^{k+1} x}\,.$$

Ihara's conjecture concerns the positivity of the constants γ_q, and it gives bounds for the ratio $\gamma_q/\log q$. In fact, it is known unconditionally

that for a density 1 set of primes q there exists a constant $c > 0$ such that

$$-c \log\log q \leq \frac{\gamma_q}{\log q} \leq 2 + \epsilon \,.$$

Assuming ERH, this property is true for all sufficiently large primes q.

Conjecture 3 (Ihara, 2009)**.** *Let $q \geq 3$ be a prime. We have:*

(i) $\gamma_q > 0$ *('very likely');*

(ii) for fixed $\epsilon > 0$ and q sufficiently large

$$\frac{1}{2} - \epsilon \leq \frac{\gamma_q}{\log q} \leq \frac{3}{2} + \epsilon \,.$$

However γ_q can be negative [1]:

$$\gamma_{964477901} = -0.1823\ldots,$$

and furthermore, assuming HL, one can prove that this happens infinitely often:

Theorem 1. *On a quantitative version of the HL conjecture we have*

$$\liminf_{q\to\infty} \frac{\gamma_q}{\log q} = -\infty \,.$$

In favour of Ihara's conjecture we have:

Theorem 2. *Under the EH conjecture, for a density 1 sequence of primes q we have*

$$1 - \epsilon < \frac{\gamma_q}{\log q} < 1 + \epsilon$$

(that is, γ_q has normal order $\log q$*).*

Sketch of proof of Theorem 1. Assume ERH and the HL conjecture. We need to find $b_1, \ldots, b_s$ such that the integers $n, 1 + b_1 n, 1 + b_2 n, \ldots$ satisfy the conditions of the HL conjecture and

$$\sum_{i=1}^{s} \frac{1}{b_i} > 2 \,.$$

We may take $\{b_i\}$ to be the sequence of *greedy prime offsets*, namely $\{2, 6, 8, 12, 18, 20, 26, \ldots\}$, and $s = 2088$. Then by the HL conjecture $q, 1+b_1 q, 1+b_2 q, \ldots, 1+b_s q$ are infinitely often all prime with $1+b_s q \leq q^2$, and so we have

$$q \sum_{\substack{p \leq q^2 \\ p \equiv 1 \bmod q}} \frac{\log p}{p-1} > q \log q \sum_{i=1}^{s} \frac{1}{b_i q} > \log q \sum_{i=1}^{s} \frac{1}{b_i} > (2 + \epsilon_0) \log q \,.$$

The proof is now concluded on invoking estimate (1). □

The *measure* of an admissible set S is defined as

$$m(S) = \sum_{s \in S} \frac{1}{s} \,.$$

Theorem 1 is a consequence of the fact that there exists an admissible set S with $m(S) > 2$. Ford, Luca and Moree gave a short proof of this fact based on a result by Erdös from 1961. However, the divergence result is due to Granville and it confirmed a conjecture of Erdös from 1988:

Theorem 3 (Granville [2])**.** *There is a sequence of admissible sets* $S_1, S_2, \ldots$ *such that* $\lim_{i \to \infty} m(S_i) = \infty$.

Proposition 1 (Granville [2])**.** *There is an admissible set S with elements $\leq x$, such that $m(S) \geq (1 + o(1)) \log \log x$. For any admissible set we have $m(S) \leq 2 \log \log x$.*

3 Analogy with Kummer's Conjecture

Kummer conjectured in 1851 that

$$h_1(q) = \frac{h(q)}{h_2(q)} \sim G(q) := 2q \left(\frac{q}{4\pi^2}\right)^{\frac{q-1}{4}},$$

where $h(q)$ and $h_2(q)$ are the class numbers of $\mathbb{Q}(\zeta_q)$ and of its maximal real subfield $\mathbb{Q}(\zeta_q)^+ := \mathbb{Q}(\zeta_q + \zeta_q^{-1})$, respectively. Define the *Kummer's ratio* as $r(q) := h_1(q)/G(q)$. Then the conjecture amounts to

$$r(q) \sim 1\,.$$

Masley and Montgomery (1976) showed that $|\log r(q)| < 7 \log q$ for $q > 200$ and used this result to determine all cyclotomic fields of class number 1. Ram Murty and Petridis (2001) showed that there exists a constant $c > 1$ such that for a density 1 set of primes q we have $1/c \le r(q) \le c$.

Both γ_q and $h_1(q)$ are related to special values of Dirichlet L-series. Hasse (1952) showed that

$$r(q) = \prod_{\chi(-1)=-1} L(1, \chi),$$

where χ runs over all the odd characters modulo q. Furthermore, using the definition of the Euler-Kronecker constant, one can find the Taylor series expansion around $s = 1$:

$$\frac{\zeta_{\mathbb{Q}(\zeta_q)}(s)}{\zeta_{\mathbb{Q}(\zeta_q)^+}(s)} = r(q)\Big(1 + (\gamma_q - \gamma_q^+)(s-1) + O_q((s-1)^2)\Big),$$

where $\gamma_q^+ := \mathcal{EK}_{\mathbb{Q}(\zeta_q)^+}$, which involves both γ_q and $h_1(q)$.

Both quantities $\log r(q)$ and $(\gamma_q - \gamma_q^+)/\log q$ are related to the distribution of primes $p \equiv \pm 1 \bmod q$. In fact, they are analytically similar in the following way

$$\frac{\gamma_q - \gamma_q^+}{\log q} \approx \frac{(q-1)}{2}\left(\sum_{\substack{p \le q(\log q)^A \\ p \equiv 1 \bmod q}} \frac{1}{p} - \sum_{\substack{p \le q(\log q)^A \\ p \equiv -1 \bmod q}} \frac{1}{p}\right) \approx \log r(q)\,. \quad (2)$$

If we assume HL and EH, then Kummer's conjecture is false. We have the following result:

Theorem 4 (Granville [2])**.** *Assume both the HL and the EH conjecture. Then $r(q)$ has $[0, \infty]$ as set of limit points.*

Similarly, in view of (2), we have that, assuming both HL and EH, the sequence $(\gamma_q - \gamma_q^+)/\log q$ can be shown to be dense in $(-\infty, \infty)$ (see [3]). In the same way, exploiting the analytic similarity of $\gamma_q/\log q$ with $1 - 2|\log r(q)|$, the sequence $\gamma_q/\log q$ is dense in $(-\infty, 1]$ (see [1]).

Exploiting these results, we obtain the following speculations, where the log log log 'devil' appears:

1. (Granville [2]) the Kummer's ratio $r(q)$ asymptotically satisfies

$$(-1 + o(1)) \log\log\log q \le 2 \log r(q) \le (1 + o(1)) \log\log\log q\,;$$

2. (Languasco, Moree, Saad Eddin, Sedunova [3])

$$(-1+o(1)) \log\log\log q \le 2\frac{(\gamma_q - \gamma_q^+)}{\log q} \le (1+o(1)) \log\log\log q\,;$$

3. (Ford, Luca, Moree [1])

$$\frac{\gamma_q}{\log q} \ge (-1 + o(1)) \log\log\log q\,.$$

These bounds are best possible in the sense that there exist infinite sequences of primes q for which all the indicated bounds are attained.

References

[1] K. Ford, F. Luca, P. Moree, *Values of the Euler ϕ-function not divisible by a given odd prime, and the distribution of Euler-Kronecker constants for cyclotomic fields*. Math. Comp. **83** (2014), 1447-1476.

[2] A. Granville, *On the size of the first factor of the class number of a cyclotomic field*. Inv. Math. **100** (1990), 321-338.

[3] A. Languasco, P. Moree, S. Saad Eddin, A. Sedunova, working paper.

Pietro Sgobba
Mathematics Research Unit
University of Luxembourg
6, Avenue de la Fonte
4364 Esch-sur-Alzette, Luxembourg.
email: pietro.sgobba@uni.lu - pietrosgobba1@gmail.com

Part II
Contributed Talks

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 5, *Number* 1, *March* 2020, *pages* 107-108

Classification of Number Fields with Minimum Discriminant

Francesco Battistoni

A classic problem in Algebraic Number Theory consists in detecting the minimum absolute value for the discriminant d_K of the number fields K having fixed degree n and fixed signature (r_1, r_2), where $n = r_1 + 2r_2$. A related topic is the research of methods to enumerate and list all the number fields of fixed degree and signature with discriminant less than a given bound.
Starting from seminal works by Minkowski and Hermite, the problem of minimum discriminant was approached during the twentieth century by means of miscellaneous techniques, from Analytic Number Theory to the study of algebraic lattices. The joint effort of many mathematicians, including Pohst, Martinet and Odlyzko, allowed to construct lists of number fields with low discriminant for any degree $n \leq 7$ and for the signatures $(8, 0), (0, 4)$ in degree 8, $(9, 0)$ in degree 9.

We present an algorithmic procedure to list all number fields of given signature with discriminant less than a specific bound. First, we introduce the main theoretical ideas on which the procedure relies: on one hand, we have results from Geometry of Numbers which show that for any number field K there is an algebraic integer α, called HPM-element of K, such that the coefficients of its minimum polynomial p_α are bounded by functions depending only on d_K and the degree n.

Thus, in order to classify the fields, we look for minimum polynomials p_α of HPM-elements α.
On the other side, we use Explicit Formulae of Dedekind Zeta functions in order to choose smart upper bounds for d_K, so that in the algorithmic procedure one can consider only number fields of given signature which do not admit prime ideals of norm ≤ 5. This arithmetical condition yields strict properties on the minimum polynomials p_α of HPM-elements α.
Finally, we combine the techniques above and we give an instance of the algorithmic procedure: we show how the aforementioned conditions allow to create a list of minimum polynomials p_α and which additional conditions they must satisfy in order to not be discarded by the algorithm.

In a joint work with B. Allombert and K. Belabas we implemented the procedure in a program running on the computer algebra PARI/GP and we used it to get minimum discriminants and fields with low discriminant for signatures $(2,3), (4,2)$ and $(6,1)$ (completing thus the degree 8 case) and signature $(1,4)$. Work on the signature $(3,3)$ is ongoing.
Although any number field given as output was previously known, the procedure showed that they are the only number fields with low discriminant for their respective signatures.

Francesco Battistoni
Dipartimento di Matematica
Università degli Studi di Milano
Via Saldini 50
20133 Milano, Italy.
email: francesco.battistoni@unimi.it

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 5, *Number* 1, *March* 2020, *pages* 109-110

Summary of results on Algebraic Geometry codes over abelian surfaces containing no absolutely irreducible curves of low genus

Yves Aubry, Elena Berardini, Fabien Herbaut & Marc Perret

We provide a theoretical study of Algebraic Geometry codes constructed from abelian surfaces defined over finite fields. We give a general bound on their minimum distance and we investigate how this estimation can be sharpened under the assumption that the abelian surface does not contain absolutely irreducible low genus curves. We state here our main results which will appear in a forthcoming paper (arXiv 1904.08227).

Theorem. *Let A be an abelian surface defined over $\mathbb{F}_q$ of trace* $\mathrm{Tr}(A)$. *Let $m = \lfloor 2\sqrt{q} \rfloor$. Then the minimum distance d of the code $C(A, rH)$ satisfies*

$$d \geq \#A(\mathbb{F}_q) - rH^2(q + 1 - \mathrm{Tr}(A) + m) - r^2 m H^2/2. \tag{1}$$

Moreover, if A is simple and contains no absolutely irreducible curves of arithmetic genus ℓ or less for some positive integer ℓ, then if $\sqrt{\frac{2\ell}{H^2}} \leq r \leq \frac{\sqrt{2}(q+1-\mathrm{Tr}(A)-m-\sqrt{\ell}(\ell-1))}{m\sqrt{H^2\ell}}$ we have

$$d \geq \#A(\mathbb{F}_q) - r\sqrt{\frac{H^2}{2\ell}}\,(q + 1 - \mathrm{Tr}(A) + (\ell - 1)m) \tag{2}$$

otherwise,

$$d \geq \#A(\mathbb{F}_q) - (q + 1 - \mathrm{Tr}(A)) - m(r^2H^2/2 - 1) - r\sqrt{\frac{H^2}{2}}(\ell - 1). \quad (3)$$

It is worth to notice that if A is simple then we can take $\ell = 1$ and that the bound (2) obtained for $\ell = 2$ improves the one obtained for $\ell = 1$ for q sufficiently large. This leads us to investigate the case of abelian surfaces with no absolutely irreducible curves of genus one nor two. We obtain the following proposition.

Proposition. *The bound on the minimum distance (2) of the previous theorem holds when taking $\ell = 2$ in the two following cases:*

1. *Let A be an abelian surface defined over $\mathbb{F}_q$ which does not admit a principal polarization. Then A does not contain absolutely irreducible curves of arithmetic genus* 0, 1 *nor* 2.

2. *Let q be a power of a prime p. Let E be and elliptic curve defined over $\mathbb{F}_{q^2}$ of Weil polynomial $f_{E/\mathbb{F}_{q^2}}(t) = t^2 - \mathrm{Tr}(E/\mathbb{F}_{q^2})t + q^2$. Let A be the $\mathbb{F}_{q^2}/\mathbb{F}_q$-Weil restriction of the elliptic curve E. Then A does not contain absolutely irreducible curves defined over $\mathbb{F}_q$ of arithmetic genus* 0, 1 *nor* 2 *if and only if one of the following cases holds:*

   a) $\mathrm{Tr}(E/\mathbb{F}_{q^2}) = 2q - 1$*;*

   b) $p > 2$ *and* $\mathrm{Tr}(E/\mathbb{F}_{q^2}) = 2q - 2$*;*

   c) $p \equiv 11 \mod 12$ *or* $p = 3$*, q is a square and* $\mathrm{Tr}(E/\mathbb{F}_{q^2}) = q$*;*

   d) $p = 2$*, q is nonsquare and* $\mathrm{Tr}(E/\mathbb{F}_{q^2}) = q$*;*

   e) $q = 2$ *or* $q = 3$ *and* $\mathrm{Tr}(E/\mathbb{F}_{q^2}) = 2q$.

Elena Berardini
Institut de Mathématiques de Marseille
Aix Marseille Université
CNRS, Centrale Marseille,
UMR 7373, France.
email: elena_berardini@hotmail.it

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 5, *Number* 1, *March* 2020, *pages* 111-112

On zero-sum subsequences in a finite abelian p-group of length not exceeding a given number

Bidisha Roy and R. Thangadurai

Let G be a finite abelian additive group with exponent $\exp(G)$. A sequence S over G of length ℓ is written as $S = (g_1, g_2, \ldots, g_\ell)$ with $g_i \in G$, not necessarily distinct. A sequence S over G of length ℓ is called a zero-sum sequence if $g_1 + g_2 + \cdots + g_\ell = 0$.

For a given positive integer $k \geq 1$, a constant $s_{\leq k}(G)$ is defined to be the least positive integer t such that given any sequence S over G of length $|S| \geq t$ contains a zero-sum subsequence of length m where m is an integer with $1 \leq m \leq k$. Then, the well-known Davenport constant, $D(G)$, is nothing but $s_{\leq |G|}(G)$ and the short zero-sum constant $\eta(G)$ is nothing but $s_{\leq \exp(G)}(G)$.

In 2010, Schmid and Zhuang [1] conjectured the following.

Conjecture 1 *([1]) Let G be a finite abelian p-group with $D(G) \leq 2\exp(G) - 1$. Then $\eta(G) = 2D(G) - \exp(G)$.*

In [2], authors proved the following result which, in particular, resolves the above conjecture for a large class of finite abelian p-groups.

Theorem 1 *[2] Let H be a finite abelian p-group with exponent $\exp(H) = p^m$ for some integer $m \geq 1$ and for a prime number $p > 2r(H)$ where*

$r(H)$ is the rank of H. Suppose the Davenport constant $D(H)$ satisfies $D(H) - 1 = kp^m + t$ for some integers $k \geq 1$ and $0 \leq t \leq p^m - 1$. Let $G = C_{p^n} \oplus H$ be a finite abelian p-group for some integer n satisfying $p^n \geq 2(D(H)-1)$. Let ℓ be any integer satisfying $\ell = ap^m + t'$ for some integer a satisfying $0 \leq a \leq k-1$ and for some integer t' satisfying $0 \leq t' \leq t$. Then, we have

$$s_{\leq \exp(G)+\ell}(G) \leq \exp(G) + 2(D(H) - 1) - \ell = 2D(G) - \exp(G) - \ell.$$

In particular, we get $\eta(G) = 2D(G) - \exp(G)$; when $H \cong C_{p^m}$ and $n \geq m+1$, for all integers $0 \leq \ell \leq p^m - 1$, we get

$$s_{\leq \exp(G)+\ell}(G) = 2D(G) - \exp(G) - \ell.$$

References

[1] W. A. Schmid and J. J. Zhuang, *O*n short zero-sum subsequences over *p*-groups, Ars. Combin., **95** (2010), 343 - 352.

[2] B. Roy and R. Thangadurai, *O*n zero-sum subsequences in a finite abelian p-group of length not exceeding a given number, J. Number Theory, **191** (2018), 246 - 257.

Bidisha Roy
Harish Chandra Research Institute, HBNI
Chhatnag Road, Prayagraj-211019, India.
email: bidisharoy@hri.res.in
R. Thangadurai
Harish Chandra Research Institute, HBNI
Chhatnag Road, Prayagraj-211019, India.
email: thanga@hri.res.in

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 5, *Number* 1, *March* 2020, *pages* 113-114

Kummer Theory for Number Fields

Antonella Perucca, Pietro Sgobba, Sebastiano Tronto

Let K be a number field, and G a finitely generated subgroup of $K^\times$ having positive rank r. We may suppose without loss of generality that G is torsion-free. For any M and N with $N \mid M$ we want to compute the degree over $K(\zeta_M)$ of the Kummer extension $K\left(\zeta_M, \sqrt[N]{G}\right)$. This degree $\deg(M, N)$ divides N^r and it is known that the quotient

$$C(M, N) := \frac{N^r}{\deg(M, N)}$$

divides a constant which is independent of M and N (a direct proof can be found in [2]). The ratio $C(M, N)$ can be seen as a failure of maximality for the Kummer extension: it is in fact the product over all prime divisors ℓ of N of two numbers, namely the *ℓ-adic failure*

$$C(\ell^n, \ell^n) = \frac{\ell^{nr}}{\left[K\left(\zeta_{\ell^n}, \sqrt[\ell^n]{G}\right) : K\left(\zeta_{\ell^n}\right)\right]}$$

where $n = v_\ell(N)$, and the *adelic failure* (with respect to ℓ)

$$\left[K\left(\zeta_{\ell^n}, \sqrt[\ell^n]{G}\right) \cap K\left(\zeta_M\right) : K\left(\zeta_{\ell^n}\right)\right] .$$

The ℓ-adic failure is explicitly computable [1]: the algorithm involves the choice of a suitable basis of G, where the generators show all the divisibility properties of G. For example, if $G = \langle 12, 18\rangle = \langle 6^3, 18\rangle$

over $\mathbb{Q}$, it is convenient to use the latter basis to compute the 3-adic failure. To control the adelic failure we make use of Schinzel's Theorem on abelian radical extensions. For example, the adelic failure for $G = \langle 5 \rangle$ is due to the fact that $\sqrt{5} \in \mathbb{Q}(\zeta_5)$.

For $K = \mathbb{Q}$, there are explicitly computable integers M_0 and N_0 such that

$$C(M, N) = C(\gcd(M, M_0), \gcd(N, N_0))$$

for all M and N. In particular there are formulas (with a case distinction) describing $C(M, N)$ for all M and N. Moreover, there is a concrete and efficient algorithm to compute these degrees for all M and N. Such an algorithm has been implemented in Sagemath by Tronto.

References

[1] C. Debry and A. Perucca: *Reductions of algebraic integers*, Journal of Number Theory, vol. 167 (2016), 259–283.

[2] A. Perucca and P. Sgobba: *Kummer Theory for Number Fields and the Reductions of Algebraic Numbers*, International Journal of Number Theory, doi:10.1142/S179304211950091X.

Antonella Perucca, Pietro Sgobba, Sebastiano Tronto
Mathematics Research Unit
University of Luxembourg
6, avenue de la Fonte
4364 Esch Luxembourg.
email: antonella.perucca@uni.lu, pietro.sgobba@uni.lu, sebastiano.tronto@uni.lu

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 5, Number 1, March 2020, pages 115-116

Statistics of moduli space of vector bundles

Sampa Dey

Let $\mathbb{F}_q$ be a finite field of characteristic p with q elements(i.e. $q = p^n$, for some positive integer n) and V be an algebraic variety defined over the algebraic closure of $\mathbb{F}_q$ denoted by $\overline{\mathbb{F}}_q$. Let $N_q(V)$ denote the number of $\mathbb{F}_q$-rational points of V. Giving an estimate of $N_q(V)$ is an active area of research in finite field theory as well as in number theory (see [2] for a recent survey on this topic).

Assume that q is odd and d is a positive integer ≥ 3. Let $\mathcal{H}_{d,q}$ be a family of curves given by the equation $y^2 = F(x)$, where F in $\mathbb{F}_q[x]$ is a degree d monic, square-free polynomial. Every such curve corresponds to an affine model of a unique projective hyperelliptic curve H with genus $g = \left[\frac{d-1}{2}\right]$. The measure on $\mathcal{H}_{d,q}$ is given by the uniform probability measure on the set of such polynomials F. Let J_H be the Jacobian of the hyperelliptic curve H which is an abelian variety of dimension g. In terms of vector bundles, one can see that J_H is the moduli space of vector bundles of rank 1 and degree 0. For a fixed g and growing q, Katz and Sarnak showed that $\sqrt{q}(\log N_q(J_H) - g \log q)$ is distributed as the trace of a random $2g \times 2g$ unitary symplectic matrix [3, Chapter 10, Variant 10.1.18]. On the other side, when the finite field is fixed and the genus g grows, Xiong and Zaharescu [4] found the limiting distribution of $\log N_q(J_H) - g \log q$ in terms of it's characteristic function and when both the genus and the finite field grow, they showed that $\sqrt{q}(\log N_q(J_H) - g \log q)$ has a standard Gaussian distribution.

We have studied similar problems for the moduli space $M_{H,L}(2,1)$ of rank 2 stable vector bundles associated to H and any degree one line bundle L on $\overline{H} = H \times_{\mathbb{F}_q} \overline{\mathbb{F}}_q$. $M_{H,L}(2,1)$ is a non-abelian, smooth projective variety of

dimension $3g-3$. We find the limiting distribution of $\log N_q(M_{H,L}(2,1)) - 3(g-1)\log q$ as g grows and q is fixed, in terms of the characteristic function and interestingly when both the genus and the size of the finite field grow we see that $q^{3/2}\left(\log N_q(M_{H,L}(2,1)) - 3(g-1)\log q\right)$ has a standard Gaussian distribution [see [1] for more details].

Theorem: If both $q, g \to \infty$,then for any H in $\mathcal{H}_{d,q}$, the quantity

$$q^{3/2}\left(\log N_q(M_{H,L}(2,1)) - 3(g-1)\log q\right)$$

is distributed as a standard Gaussian. More precisely, for any x in $\mathbb{R}$ we have,

$$\lim_{\substack{q\to\infty \\ g\to\infty}} \frac{1}{\#\mathcal{H}_{d,q}} \#\left\{H \in \mathcal{H}_{d,q} : q^{3/2}\left(\log N_q(M_{H,L}(2,1)) - 3(g-1)\log q\right) \le x\right\} = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{x} e^{-t^2/2}dt.$$

References

[1] A. Dey, S. Dey and A. Mukhopadhyay, *Statistics of moduli space of vector bundles*, Bull. Sci. Math. 151(2019), 13–33.

[2] S. R. Ghorpade and G. Lachaud, *Number of solutions of equations over finite fields and a conjecture of Lang and Weil,* Number theory and discrete mathematics (Chandigarh, 2000), 269–291.

[3] N. M. Katz and P. Sarnak, *Random matrices, Frobenius eigenvalues, and monodromy,* American Mathematical Society Colloquium Publications, American Mathematical Society, Providence, RI, 45(1999).

[4] M. Xiong and A. Zaharescu, *Statistics of the Jacobians of hyperelliptic curves over finite fields*, Math. Res. Lett. 19 (2012), 255–272.

Sampa Dey
Department of Mathematics
Indian Institute of Technology Madras
IIT P.O.
Chennai 600 036 INDIA.
email: sampa.math@gmail.com

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 5, *Number* 1, *March* 2020, *pages* 117-118

Approximations by Signed Harmonic Sums and the Thue–Morse Sequence

Sandro Bettin, Giuseppe Molteni, Carlo Sanna

We study how well a real number τ can be approximated by *signed harmonic sums*, that is, sums of the form

$$\sum_{m=1}^{n} \frac{s_m}{m},$$

where $s_1, \dots, s_n \in \{-1, +1\}$.

A first approach consists of understanding how much small can be the following quantity

$$\mathfrak{m}_n(\tau) := \min\left\{\left|\tau - \sum_{m=1}^{n} \frac{s_m}{m}\right| : s_1, \dots, s_n \in \{-1, +1\}\right\},$$

as $n \to +\infty$. In this direction, we proved the following result:

Theorem 1 *For all $\tau \in \mathbb{R}$ and $\varepsilon > 0$, we have*

$$\mathfrak{m}_n(\tau) < \exp\left(-\left(\tfrac{1}{\log 4} - \varepsilon\right)(\log n)^2\right),$$

for all sufficiently large positive integers n, depending on τ and ε.

A second approach consists of choosing the sequence of signs "greedily". Precisely, for every $\tau \in \mathbb{R}$, we define

$$\sigma_n(\tau) := \sum_{m=1}^{n} \frac{s_m(\tau)}{m} \quad \text{and} \quad s_n(\tau) := \begin{cases} +1 & \text{if } \tau \geq \sigma_{n-1}(\tau) \\ -1 & \text{if } \tau < \sigma_{n-1}(\tau) \end{cases}$$

for all integers $n \geq 0$ (with the convention $\sigma_0(\tau) := 0$). It is not difficult to see that $\sigma_n(\tau) \to \tau$, as $n \to +\infty$. More precisely, $|\sigma_n(\tau) - \tau| \leq 2/(n+1)$ for all n following the first sign change. More interestingly, we prove the following:

Theorem 2 *We have*

$$\liminf_{n \to +\infty} \frac{\log |\tau - \sigma_n(\tau)|}{(\log n)^2} = -\frac{1}{\log 4},$$

for almost all $\tau \in \mathbb{R}$, respect to Lebesgue measure.

Carlo Sanna
Department of Mathematics
Università di Genova
Via Dodecaneso, 35
16146 Genova, Italy.
email: carlo.sanna.dev@gmail.com

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 5, *Number* 1, *March* 2020, *pages* 119-120

Multidimensional p-adic continued fractions

Nadir Murru, Lea Terracini

Given a m-tuple of real numbers as input, the Jacobi–Perron (JP) algorithm returns m sequences of integers. We define the p-adic JP algorithm as follows: given $(\alpha_0^{(1)}, ..., \alpha_0^{(m)})$ in $\mathbb{Q}_p^m$,

$$a_n^{(i)} = s(\alpha_n^{(i)}), \quad \alpha_{n+1}^{(1)} = \frac{1}{\alpha_n^{(m)} - a_n^{(m)}}, \quad \alpha_{n+1}^{(i)} = \frac{\alpha_n^{(i-1)} - a_n^{(i-1)}}{\alpha_n^{(m)} - a_n^{(m)}},$$

where s is the *Browkin floor function*, defined by $s(\alpha) - \alpha \in p\mathbb{Z}_p$, $s(\alpha) \in \mathbb{Z} \cap \left[\frac{1}{p}\right] \cap \left(-\frac{p}{2}, \frac{p}{2}\right)$. The output sequences $[(a_n^{(1)})_{n=0}^{\infty}, ..., (a_n^{(m)})_{n=0}^{\infty}]$ represent a multidimensional continued fraction (MCF) converging to the starting m–tuple and they satisfy the *convergence conditions* $|a_n^{(1)}|_p > 1$, for $n \geq 1$, $|a_n^{(i)}|_p < |a_n^{(1)}|_p$, for $i = 2, \ldots, m+1, n \geq 1$. Concerning finiteness and rational dependence, we proved:

Theorem 1 *Assume that* $(\alpha_0^{(1)}, \ldots, \alpha_0^{(m)}) \in \mathbb{Q}^m$. *Then the p-adic JP-algorithm stops in a finite number of steps (bounded by* $ht(\alpha_0^{(1)}, \ldots, \alpha_0^{(m)})$.

Theorem 2 *Assume* $m = 2$ *and* $(\alpha, \beta, 1)$ *linearly dependent over* $\mathbb{Q}$ *: if the p-adic JP-algorithm does not stop then* $v_p(a_n) = -1$ *for infinitely many n.*

Conjecture 1 *If* $(\alpha_0^{(1)}, ..., \alpha_0^{(m)}, 1)$ *are linearly dependent over* $\mathbb{Q}$ *then the associated p-adic MCF is either finite or periodic.*

We also investigated periodicity; consider a purely periodic MCF of period N, i.e., $a_{(k+N)}^{(i)} = a_k^{(i)}$ for every $k \in \mathbb{N}$, and define

$$\mathcal{M} = \mathcal{A}_0\mathcal{A}_1 \dots \mathcal{A}_{N-1}, \text{ where } \mathcal{A}_n = \begin{pmatrix} a_n^{(1)} & 1 & 0 & \dots & 0 \\ a_n^{(2)} & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_n^{(m)} & 0 & 0 & \dots & 1 \\ 1 & 0 & 0 & \dots & 0 \end{pmatrix}.$$

Then $(\alpha_0^{(1)}, \dots, \alpha_0^{(m)}, 1)$ is an eigenvector for $\mathcal{M}$. Let $\mu \in \overline{\mathbb{Q}}_p$ be the associated eigenvalue, and $P(X)$ be the characteristic polynomial. We proved

- μ is a strictly dominant eigenvalue of $\mathcal{M}$, and every root of P in $\overline{\mathbb{Q}}_p$ other than μ has p-adic norm < 1.
- $\mathbb{Q}(\mu) = \mathbb{Q}(\alpha^{(1)}, \dots, \alpha^{(m)})$ and $\mu \notin \mathbb{Q}$.
- If $N = 1$ then P does not have any root in $\mathbb{Q}$.
  If $m = 2$ and $N = 2$ then P is irreducible over $\mathbb{Q}$ unless the following conditions are verified: one between a_0 and a_1 (say a_0) is of the form $\pm\frac{1}{p} + w$ with $w \in \mathbb{Z}, |w| \leq \frac{p-1}{2}, w \neq 0$; and either $v(a_1 p + 1) = v(a_1) + 1$ or a_1 is of the form $\pm\frac{1}{p} + u$ with $u \in \mathbb{Z}, |u| \leq \frac{p-1}{2}, u \neq 0$.

The last fact allows to provide examples of p-adic $\mathbb{Q}$-linearly dependent p-adic pairs with infinite periodic MCF.

Nadir Murru, Lea Terracini
Dipartimento di Matematica
Università di Torino
Via Carlo Alberto 10
10123 Torino (Italy).
email: nadir.murru@unito.it, lea.terracini@unito.it

PREVIOUS PUBLICATIONS OF THE PROCEEDINGS

Proceedings of the 1st mini symposium of the Roman Number Theory Association. Università Europea di Roma (May 7th, 2015), edited by Marina Monsurrò, Francesco Pappalardi, Valerio Talamanca, Roma 2016, cm. 14,8x21, 84 pp., ISBN 978-88-6788-077-5.

Proceedings of the 2nd mini symposium of the Roman Number Theory Association. Università degli Studi Roma Tre (April 26th, 2016), edited by Marina Monsurrò, Francesco Pappalardi, Valerio Talamanca and Alessandro Zaccagnini, Roma 2017, cm. 14,8x21, 96 pp., ISBN 978-88-6788-113-0.

Proceedings of the 3rd mini symposium of the Roman Number Theory Association. Università degli Studi Roma Tre (April 6th, 2017), edited by Marina Monsurrò, Francesco Pappalardi, Valerio Talamanca and Alessandro Zaccagnini, Roma 2018, cm. 14,8x21, 82 pp., ISBN 978-88-6788-140-6.

Proceedings of the 4th mini symposium of the Roman Number Theory Association. Università degli Studi Roma Tre (April 18-20th, 2018), edited by Marina Monsurrò, Francesco Pappalardi, Valerio Talamanca and Alessandro Zaccagnini, Roma 2019, cm. 14,8x21, 160 pp., ISBN 978-88-6788-171-0.

Proceedings of the 5th mini symposium of the Roman Number Theory Association. Università Roma Tre (April 10th-12th, 2019), edited by Fabrizio Barroero, Marina Monsurrò, Francesco Pappalardi, Valerio Talamanca and Alessandro Zaccagnini, Roma 2021, cm. 14,8x21, 136 pp., ISBN 978-88-6788-267-0.

Finito di stampare nel mese di dicembre 2021
da IF Press srl
Stampato in Italia - Printed in Italy