Proceedings of the 4th mini symposium of the Roman Number Theory Association

Università Roma Tre

April 10th-12th, 2018

Contents

Foreword

This volume contains the proceedings of the Fourth mini symposium of the Roman Number Theory Association. The conference was held on April 18-20, 2018 at the Università degli Studi Roma Tre.This symposium was a milestone for RNTA: for the first time, the duration was of three days and we also hosted, as a satellite conference, the 11th 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 ALGANT Consortium, CNRS-GDRI, LYSM “Ypatia Laboratory of Mathematical Sciences”, the department of Mathematics and Physics of the Università Roma Tre, the Università Europea di Roma and the Università Roma Tre for funding the event.

The Roman Number Theory Association

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

This conference, whose proceedings are collected here, represents the evidence of our goal: to be a key player in the development of a strong Roman community of number theorists, to foster a specific scientific program but also, and more importantly, to create a framework

of opportunities for scientific cooperation for anyone interested in number theory. Among these opportunities we can enlist the Scriba project as well as the international cooperation with developing countries and the support of young researcher in number theory with special regards to those coming from developing countries.

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

Our statute is available on the association's website (www.rnta.eu) and it clearly states that our efforts and our funds will be devoted entirely to the development of Number Theory. This will be achieved in several ways: by directly 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 five years, the Roman Number Theory Association has been involved in many different activities, here the list of the most recent and significant.

The Fifth mini Symposium of the association will take place on 10-12 April 2019 and, again, have a duration of three days; we will also host again, as a satellite conference, the 12th PARI/GP Atelier. The annual symposium represents for us a very special moment to bring together most people involved in RNTA and especially our Advisory Board. The scriba project is already launched for this symposium as well.

Besides, the Association collaborated in various ways to other events in 2018 and 2019, namely

- *13th Atelier PARI/GP*, Università Roma Tre, April 8-9, 2019;
- *The Eleventh International Conference on Science and Mathematics Education in Developing Countries*, The National University of Laos, Laos, held in November 2018;
- *11th Atelier PARI/GP*, Università Roma Tre, April 16-17, 2018;

Another very important engagement of the association is the organisation of 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 *Group Actions in Arithmetic and Geometry*, Universitas Gadjah Mada Yogyakarta, Indonesia, February 17-28, 2020
- 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 República, Montevideo, Uruguay, February 11 - 22, 2019.
- WAMS research school on *Representation Theory*, College of Science, University of Sulaymaniyah, Sulaymaniyah, Kurdistan Region, Iraq, February 7 - 9, 2019
- Emil Artin International School in Mathematics for Students and WAMS research school on *The Mathematics of Artin's conjectures*, Yerevan State University, Yerevan, Armenia May 21 - 25, 2018
- CIMPA research school on *Arithmétique algorithmique et cryptographie*. Université de Kinshasa, Kinshasa, Democratic Republic of Congo, May 7 - 18, 2018.
- CIMPA research school on *Explicit Number Theory*, The Witwatersrand University, Johannesburg, South Africa, January 8th-19th, 2018;
- WAMS research school on *Topics in Analytic and Transcendental Number Theory*, Institute for Advanced Studies in Basic Sciences (IASBS) Zanjan, Iran, to be held in July 1 - July 13 2017;

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

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

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

The Association also promotes, organizes and 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, collaborated 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 consortium (ALGANT);
10. Università Roma Tre;
11. Università Europea di Roma.

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

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

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

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

Participants

1. Oleksiy Klurman *(Kungliga tekniska högskola)*
2. Bayarmagnai Gombodorj *(National University of Mongolia)*
3. Remis Tonon *(Università di Parma)*
4. Mattia Cafferata *(Università di Parma)*
5. Giamila Zaghloul *(Università di Genova)*
6. Angelo Iadarola *(Université de Lille)*
7. Amir Akbary *(University of Lethbridge)*
8. Dario Antolini *(Università di Roma Tor Vergata)*
9. Alp Bassa *(Boğaziçi Üniversitesi)*
10. Eduardo Ruiz Duarte *(Rijksuniversiteit Groningen)*
11. Lorenzo Benedini *(Università di Pisa)*
12. Tomoko L. Kitagawa *(Historian of Mathematics, Oxford)*
13. Peter Stevenhagen *(Universiteit Leiden)*
14. Lorenzo Pagani *(Sapienza Università di Roma)*
15. Alejandro Giangreco Maidana *(Aix-Marseille Université)*
16. Evelina Viada *(Georg-August-Universität Göttingen)*
17. Antonella Perucca *(University of Luxembourg)*
18. Marina Monsurrò *(RNTA and Università Europea di Roma)*
19. Adriana Salerno *(Bates College)*
20. Chantal David *(Concordia University)*
21. René Schoof *(Università di Roma Tor Vergata)*
22. Hester Graves *(Institute of Defense Analyses)*
23. Elena Berardini *(Aix-Marseille Université)*
24. Christophe Ritzenthaler *(Université de Rennes 1)*
25. Daniele Mastrostefano *(University of Warwick)*
26. Nasreddine Benbelkacem *(Université des Sciences et de la Technologie Houari Boumediene)*

27. Pietro Corvaja *(Università di Udine)*
28. Pieter Moree *(Max-Planck-Institute for Mathematics)*
29. Florian Luca *(Wits University)*
30. Hamza Moufek *(Université des Sciences et de la Technologie Houari Boumediene)*
31. Bouazzaoui Zakariae *(Université Molay Ismaïl)*
32. Ilaria Del Corso *(Università di Pisa)*
33. Stevan Gajovic *(Rijksuniversiteit Groningen)*
34. Alessandro Zaccagnini *(Università di Parma)*
35. Mohamed Anwar Mohamed Fouad *(Università Roma TRE)*
36. Stefano Marseglia *(Stockholms universitet)*
37. Ade Irma Suriajaya *(RIKEN, Tokyo)*
38. Bouzidi Ahmed Djamal Eddine *(Université des Sciences et de la Technologie Houari Boumediene)*
39. Leonardo Zapponi *(Sorbonne Université, Paris)*
40. Alberto Perelli *(Università di Genova)*
41. Francesco Battistoni *(Università di Milano)*
42. Francesco Amoroso *(Université de Caen)*
43. Marine Rougnant *(Université de Franche-Comté)*
44. Marco Cantarini *(Università di Parma)*
45. Victoria Cantoral Farfan *(International Center for Theoretical Physics)*
46. Manh Hung Tran *(Chalmers Tekniska Högskola)*
47. Youssouf Akrour *(University Mouhamed Sedik Ben Yahia)*
48. Alessandro Gambini *(Università di Parma)*
49. Linda Frey *(Universität Basel)*
50. Bill Allombert *(CNRS/Université de Bordeaux)*
51. Abdelaziz El Habibi *(Université Mohammed Premier Oujda)*
52. Fabio Caldarola *(Università della Calabria)*
53. Giovanni Coppola *(Università di Salerno)*
54. Zouhair Boughadi *(Université Molay Ismaïl)*
55. Valerio Talamanca *(RNTA and Università Roma TRE)*
56. Laura Capuano *(University of Oxford)*
57. Nadir Murru *(Università di Torino)*
58. Abdelillah Jamous *(Université des Sciences et de la Technologie Houari Boumediene)*

59. Carlo Sanna *(Università di Torino)*
60. Guido Lido *(University of Roma "Tor Vergata")*
61. Dimitrios Chatzakos *(Université de Lille)*
62. Subramani Muthukrishnan *(Harish Chandra Research Institute)*
63. Peter Lombaers *(Universidade do Porto)*
64. Pranendu Darbar *(Institute of Mathematical Sciences)*
65. Giacomo Cherubini *(Università di Genova)*
66. Boualem Sadaoui (Université de Khemis Miliana)
67. Eda Kırımli *(Boğaziçi Üniversitesi)*
68. Andam Mustafa *(Salahahddin University-Erbil)*
69. Alessandro Murchio *(Aix-Marseille Université)*
70. Manoj Gyawali *(Università Roma TRE)*
71. Christian Maire *(Université Bourgogne Franche-Comté)*
72. Farzad Aryan *(Georg-August-Universität Göttingen)*
73. Francesco Pappalardi *(RNTA and Università Roma TRE)*
74. Michel Waldschmidt *(Sorbonne Université, Paris)*
75. Salah Eddine Rihane *(Université des sciences et de la technologie Houari Boumediene)*

Other participants (not in the photo)

- Andrea Surroca
- Andrei Yafaev *(University College London)*
- Aurel Page *(INRIA Bordeaux Sud Ouest)*
- Benseba Boualem *(Université des Sciences et de la Technologie Houari Boumediene)*
- Elisa Lorenzo Garcia *(Université de Rennes 1)*
- Fabrizio Barroero *(Universität Basel)*
- Orchidea Maria Lecian *(Sapienza Università di Roma)*
- Marco Pedicini *(Università Roma TRE)*
- Mohammed Bouhadji *(Université Oran)*
- Pietro Mercuri *(Sapienza Università di Roma)*
- Sumaia Saad Eddin *(Johannes Kepler Universität Linz)*


1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75

Part I

The Scriba Project

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 4, *Number* 1, *March* 2019, *pages* 3-8

Alp Bassa

Rational point on curves over finite fields and Drinfeld modular varieties

Written by Dario Antolini

Let's consider C a smooth projective absolutely irreducible curve over a finite field $\mathbb{F}_q$ (shortly, a *curve*). As usual, one can associate to C a Zeta function together with a corresponding Riemann Hypothesis, which we know to be true thanks to the result of Hasse–Weil.

In particular, they gave us the so-called Hasse–Weil bound for the number of $\mathbb{F}_q$-rational points of C:

$$\#C(\mathbb{F}_q) \leq q + 1 + 2g(C)\sqrt{q}, \tag{1}$$

where $g(C)$ denotes the genus of the curve C. Here, we write down just the upper bound because, as the genus increases over a fixed finite field, the lower bound becomes useless.

A first improvement of this bound was given by Ihara ([6]). Starting from the inequality

$$\#C(\mathbb{F}_{q^2}) \geq \#C(\mathbb{F}_q),$$

together with the Weil conjectures, he showed that the upper bound (1) is not good as $g(C) \gg 0$.

Moreover, Ihara considered the following quantity:

$$A(q) := \limsup_{g(C)\to\infty} \frac{\#C(\mathbb{F}_q)}{g(C)}$$

where the lim sup is taken over all the curves C over the (fixed) field $\mathbb{F}_q$ when $g(C)$ tends to infinity. He showed that the number $A(q)$ always exists and depends only on the base field $\mathbb{F}_q$. Thus, from the Hasse–Weil bound (1), we have

$$A(q) \leq 2\sqrt{q}.$$

An important result on these side was given by Drinfeld and Vlăduţ ([3]) proving that

$$A(q) \leq \sqrt{q} - 1, \tag{2}$$

and this bound is the best known since 1983.

Conversely, the lower bound case was (historically) more difficult.

The first result is due to Serre ([7]) showing that the number $A(q)$ is always nonzero:

$$A(q) > 0,$$

while Ihara ([5]) specilized in the case $q = l^2$, with l prime power, obtaining:

$$A(q) \geq \sqrt{q} - 1. \tag{3}$$

So, by comparison with (2), we can conclude the equality:

$$A(l^2) = l - 1.$$

The last improvement on this side is given by Zink ([8]) when $q = p^3$ and it states the following inequality:

$$A(p^3) \geq \frac{2(p^2 - 1)}{p + 2}. \tag{4}$$

On proving his result (3), Ihara considered a sequence of Shimura curves over a same base field with increasing genus. Let's sketch the main ideas due to Ihara in the case of modular curves.

Let N be a positive integer. Denote by $X_0(N)$ the modular curve with $\Gamma_0(N)$-structure, where the affine locus (non-cuspidal points) parametrizes isomorphism classes of elliptic curves over $\mathbb{C}$ (also over $\overline{\mathbb{Q}}$) together with a cyclic N isogeny. It is a well-known result that $X_0(N)$ can be described over $\mathbb{Q}$, and, furthermore, after the work of Deligne–Rapoport ([2]), it has a (smooth projective irreducible) model in $\mathbb{Z}[1/N]$. Hence, for every prime number $p \nmid N$, we can reduce $X_0(N)$ mod p and obtain a (irreducible) curve $\widetilde{X_0}(N)$ over $\mathbb{F}_p$.

Moreover, this curve classifies the isomorphism classes of elliptic curves over $\overline{\mathbb{F}_p}$ + additional structure (and cusps). The interesting fact is that $\widetilde{X_0}(N)$ has many $\mathbb{F}_{p^2}$-points, whose non-cuspidal points correspond to the so-called supersingular elliptic curves.

Now, let's consider an increasing sequence of positive integers $\{N_i\}$, with $p \nmid N_i$ for all i and $N_i \to \infty$ as $i \to \infty$. Then, Ihara proved that

$$\lim_{i\to\infty} \frac{\#\widetilde{X_0}(N_i)(\mathbb{F}_{p^2})}{g(\widetilde{X_0}(N_i))} = p - 1$$

by using computations involving Shimura curves.

Now, let's point out the key points on the proof. In particular, why do we get just a result for $\mathbb{F}_{p^2}$-points and not other extensions of $\mathbb{F}_p$?

What Ihara was able to discover is the existence of $\mathbb{F}_{p^2}$-points in the modular curves $\widetilde{X_0}(N_i)$, in particular of supersingular elliptic curves. It is well-known that their j-invariant lie inside $\mathbb{F}_{p^2}$, and one obtains exactly this degree-2 extension because the modular curve parametrizes (isomorphism classes of) elliptic curves over $\mathbb{C}$ as well as $\mathbb{Z}$-lattices of rank 2 inside $\mathbb{C}$ (up to homothety).

So, in order to generalize this bound for $q = l^n$ with l prime integer and $n > 2$, one has to look at lattices of rank n, but inside another algebraically closed field, since the field complex numbers offer us just rank-2 lattices. (We cannot consider rank-1 lattices because their moduli space will be 0-dimensional.) First, replace the integers $\mathbb{Z}$ inside its fraction field $\mathbb{Q}$ by the ring $A := \mathbb{F}_q[T]$ inside the field $F := \mathbb{F}_q(T)$; hence, consider its completion F_∞ at the ∞ place and its algebraic

closure $\overline{F_\infty}$. Since this extension is of infinite degree, the latter is no more complete, meanwhile its completion C_∞ is still algebraically closed.

In this equal-characteristic setting, we need an analogue of the elliptic curve: it is called Drinfeld module, and it can be shown ([4, Theorem 4.6.9]) that the moduli space of (isomorphism classes of) Drinfeld modules with rank n is equivalent to the moduli spaces of A-lattices of rank n inside C_∞ (up to homothety), as far as for elliptic curve (with $n = 2$).

In a similar way, one can define a level structure on Drinfeld modules: it turns out that the moduli space of rank-n Drinfeld modules together with (nontrivial) level structure can be represented by an $(n-1)$-dimensional affine scheme $\mathcal{M}$ over A. Then, as in the elliptic curve case, we want to reduce this scheme modulo a prime element of A. In this case, we look for an ideal "not intersecting the level structure" (in some sense, like $V(p)$ does not intersect $V(N)$ for $p \nmid N$ inside Spec $\mathbb{Z}$), and this is generated by a polynomial $P(T) \in A = \mathbb{F}_q[T]$, since the ring A is a PID. The reduction modulo this ideal gives us a representable moduli space $\widetilde{\mathcal{M}}$ of dimension $n-1$ with many $\mathbb{F}_{p^n}$-rational points over a degree-n extension of $\mathbb{F}_q[T]/(P(T))$. Finally, there is a similar notion of supersingular Drinfeld modules and they are defined over this extension of degree n.

Let's come back to Ihara's trick. Consider a family of moduli spaces of rank-n Drinfeld modules $\{\mathcal{M}_i\}_i$ with nontrivial level structure and a polynomial $P(T)$ not intersecting any of these level structures. So, it makes sense to consider the family $\{\widetilde{\mathcal{M}_i} := \mathcal{M}_i \mod P\}$ given by reduction modulo the (ideal generetad by) $P(T)$. Starting with the scheme $\widetilde{\mathcal{M}_1}$, look at a supersingular point inside it and a *suitable* curve passing through this special point, where suitable means that it is (and can be) chosen so that it contains many supersingular points. Then, pull back this curve to the schemes $\widetilde{\mathcal{M}_i}$ and get other nice curves, so that one has a family of 1-dimensional sub-locus containing supersingular points.

Beside this theory, in [1] Bassa, Beelen, Garcia and Stichtenoth write down explicit recursive equations for these nice curves. In this way, they get a lower bound for $A(q)$ when $q = p^{2m+1}$ is an odd power of a prime number p (and $m \geq 1$). They indeed find a sort of harmonic average between two successive Drinfeld–Vlăduţ upper bounds (2):

$$A(p^{2m+1}) \geq \frac{2}{\frac{1}{p^m-1} + \frac{1}{p^{m+1}-1}}. \tag{5}$$

In particular, This lower bound can recover Zink's inequality (4) just setting $m = 1$ (so that $q = p^3$).

Last, we want to mention some applications of this result. After the historical Hasse–Weil bound, the problem of finding curves with many rational points becomes again important (ACTUAL) after the formulation of codes theory and the Goppa's construction of good codes, as long as other applications to cryptography.

In a theoretical side, this result can be used on the study of automorphisms and level structures of those curves, and also on their covering (in this case, not Galois).

References

[1] A. Bassa, P. Beelen, A. Garcia and H. Stichtenoth, *Towers of function fields over non-prime finite fields*. Mosc. Math. J. 15 (2015), no. 1, 1–29, 181.

[2] P. Deligne and M. Rapoport, *Les schémas de modules de courbes elliptiques*. In: *Modular functions of one variable II*. Springer, Berlin, Heidelberg, 1973. p. 143-316.

[3] V.G. Drinfeld and S.G. Vlăduţ, *The number of points of an algebraic curve*. Funktsional Anal. i Prilozhen 17, 68-69, 1983.

[4] D. Goss, *Basic structures of function field arithmetic*. Springer Science & Business Media, 2012.

[5] Y. Ihara, *Congruence relations and Shimura curves*. Automorphic forms, representations and L-functions, Sympos. Pure Math., Oregon State Univ. 1977, Proc. Sympos. Pure Math., XXXIII, Amer. Math. Soc., Providence, R.I., 291-311 (1979).

[6] Y. Ihara, *Some remarks on the number of rational points of algebraic curves over finite fields*. J. Fac. Sci. Tokyo 28, 721-724, 2000.

[7] J.-P. Serre, *Sur le nombre des points rationnels dâĂŹune courbe algebrique sur un corps fini*. C.R. Acad. Sc. Paris 296, 397-402, 1983.

[8] T. Zink, *Degeneration of Shimura surfaces and a problem in coding theory*. Fundamentals of Computation Theory (ed. L.Budach), Lecture Notes Comp. Sc. LNCS 199, 503-511 (1985).

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 4, *Number* 1, *March* 2019, *pages* 9-15

Peter Stevenhagen

On Redei's reciprocity law

Written by Francesco Battistoni

1 Quadratic reciprocity law

Since their discover, reciprocity laws have been a very powerful tool in Number Theory, because of their theoretical meaning and their practical usefulness. The first instance of these laws is the Quadratic Reciprocity Law, which was proved by Gauss in [3].
Let p be an odd prime number and $a \in \mathbb{Z}$ coprime with p. The Legendre symbol is defined as:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a square mod } p; \\ -1 & \text{otherwise.} \end{cases}$$

The reciprocity we refer to lies in the fact, proved by Gauss, that the Legendre Symbol is "essentially symmetric", in the following sense:

Theorem 1 (Quadratic Reciprocity Law) *Let p and q be two distinct odd prime numbers. Then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

One can obtain the following generalization: let a, b be coprime integers, and define the Jacobi symbol as:

$$\left(\frac{a}{b}\right) = \prod_{p \nmid 2a} \left(\frac{a}{p}\right)^{\mathrm{ord}_p(b)}.$$

Theorem 2 *Let a, b be two odd coprime integers. Then*

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2}\frac{b-1}{2}}(-1)^{\frac{\mathrm{sign}(a)-1}{2}\frac{\mathrm{sign}(b)-1}{2}}. \tag{1}$$

2 Hilbert symbols

A similar statement can be proved also for generic number fields, using some knowledge of Class Field Theory.
Let K be a number field, $\mathfrak{P}$ a prime of K (either finite or infinite) and $K_{\mathfrak{P}}$ the completion. Let $L := K_{\mathfrak{P}}\left(\sqrt{K^*_{\mathfrak{P}}}\right)$ be the maximal abelian extension of $K_{\mathfrak{P}}$ of exponent 2. Given $a, b \in K^*_{\mathfrak{P}}$, we define the Hilbert symbol at $\mathfrak{P}$ as:

$$(a, b)_{\mathfrak{P}} := \frac{\sigma_a(\sqrt{b})}{\sqrt{b}} \in \{\pm 1\}$$

where $\sigma_a \in \mathrm{Gal}(L/K_{\mathfrak{P}})$ is the Artin symbol of a. From Class Field Theory we get the following:

Theorem 3 (Universal Quadratic Reciprocity Law) *Let K be a number field, $a, b \in K^*$. Then $(a, b)_{\mathfrak{P}} = 1$ for almost every $\mathfrak{P}$ and*

$$\prod_{\mathfrak{P} \leq \infty} (a, b)_{\mathfrak{P}} = 1.$$

This statement generalizes the Reciprocity Law expressed in (1): in fact, when $K = \mathbb{Q}$, the odd primes properly dividing a and b give the Legendre symbols, while the right hand side is given by $(a, b)_2$ and $(a, b)_\infty$.

3 Motivation: 2^k-rank of class groups

Let $K := \mathbb{Q}(\sqrt{D})$ be a quadratic field of discriminant D, and let C be its narrow class group. It is known since Gauss that this group is of great importance in Number Theory, especially because of its connection with binary quadratic forms, and therefore it has been widely studied. Gauss himself understood that it was easier to deal with the 2-part of this group, and discovered the following:

Theorem 4 (Genus Theory) *Write $D = \prod_{i=1}^{t} d_i$, with d_i either a signed prime $\pm p \equiv 1$ mod 4 or an element of $\{4, \pm 8\}$. For every $i = 1, \dots, t$, let $\mathfrak{d}_i$ be the prime ideal of K dividing d_i.*
Then $\#C/C^2 = \#C[2] = 2^{t-1}$ and $C[2]$ is generated by the classes $[\mathfrak{d}_i]$'s modulo a single relation.

Define the 2^k-rank of an abelian group A as $r_{2^k} := \dim_{\mathbb{F}_2} A[2^k]/A[2^{k-1}]$. The theorem above characterizes the 2-rank of the class group C.
The study of the 4-rank of C required more instruments, and the first results were obtained by Redei [5], by means of Class Field theory: in fact, $C/C^2 \simeq \mathrm{Gal}(G/K)$ where $G := K(\sqrt{d_1}, \dots, \sqrt{d_t})$ is the maximal finitely unramified abelian extension of K which is abelian also over $\mathbb{Q}$. Using the natural morphism $\phi : C[2] \to C/C^2$, we define a map R via the commutative diagram:

$$\begin{array}{ccc} \mathbb{F}_2\mathfrak{d}_1 \oplus \cdots \oplus \mathbb{F}_2\mathfrak{d}_t & \xrightarrow{R} & \mathrm{Gal}(G/\mathbb{Q}) \simeq \prod_{j=1}^{t} \mathrm{Gal}(\mathbb{Q}(\sqrt{d_j})/\mathbb{Q}) \\ \downarrow & & \uparrow \\ C[2] & \xrightarrow{\phi} & C/C^2 \simeq \mathrm{Gal}(G/K). \end{array}$$

The combination of the map ϕ and of the Artin isomorphism implies that the map R (called the Redei map) is described by a matrix (c_{ij}) whose entries are connected to the action of the Artin symbol of $\mathfrak{d}_i$ on

$\sqrt{d_j}$. When $i \neq j$, in fact, the computation of the c_{ij}'s is brought back to Legendre symbols in the following way:

$$\text{for } d_i \text{ odd:} \qquad (-1)^{c_{ij}} = \left(\frac{d_j}{d_i}\right);$$

$$\text{for } d_i \text{ even:} \qquad c_{ij} = 0 \quad \text{if 2 splits in } \mathbb{Q}(\sqrt{d_j}), \quad c_{ij} = 1 \text{ otherwise.}$$

Finally, c_{ii} is chosen in order to have $\sum_j c_{ij} = 0$ in $\mathbb{F}_2$. This setting leads to the following:

Theorem 5 *Let r_4 be the 4-rank of C. Then $r_4 = t - 1 - rank_{\mathbb{F}_2} R$.*

The study of the 8-rank of C requires even more efforts: it was originally started by Redei himself in [6]. The result was achieved via the definition of a new symbol, which is seen to satisfy a new reciprocity law.

4 Redei's symbol and Redei's reciprocity law

Let $a, b, c \in \mathbb{Z}$ squarefree integers $\neq 1$ satisfying:

A) $(a,b)_p = (a,c)_p = (b,c)_p = 1 \qquad \forall p \leq \infty$;

B) $S(a) \cap S(b) \cap S(c) = \emptyset$ where $S(x) := \{p\colon p \text{ ramifies in } \mathbb{Q}(\sqrt{x})/\mathbb{Q}\}$.

Condition A) implies that $x^2 - ay^2 - bz^2 = 0$ has a non-trivial solution (x, y, z) in $\mathbb{Q}$. Let $\beta := x + y\sqrt{a}$ and define $K := \mathbb{Q}(\sqrt{ab})$, $L := \mathbb{Q}(\sqrt{a},\sqrt{b})$, $F := L(\sqrt{\beta})$. F is a cyclic extension of K with degree 4, and a dihedral extension of $\mathbb{Q}$ with degree 8.
Denote with $\Delta(a)$ and $\Delta(b)$ the discriminants of $\mathbb{Q}(\sqrt{a})$ and $\mathbb{Q}(\sqrt{b})$ respectively.

Lemma 1 *The field F as above can be chosen such that:*

- *F is unramified outside $S(a) \cup S(b)$;*

- *F is unramified over 2 whenever $\Delta(a)\Delta(b)$ is odd, or one of $\Delta(a), \Delta(b)$ is 1 mod 8;*
- *If the pair $(\Delta(a), \Delta(b))$ is equal to $(4,5)$ or $(5,4)$ mod 8, then the local extension $\mathbb{Q}_2(\sqrt{a}) \subset F \otimes \mathbb{Q}_2$ is of conductor 2;*
- *$\forall \mathfrak{c}$ integral ideal of K with norm $|c|$, the Artin symbol $Art_{\mathfrak{c},F/K}$ is in $\mathrm{Gal}(F/L) \simeq \{\pm 1\}$ and does not depend on the choice of $\mathfrak{c}$.*
- *If $a, b > 0$, for every infinite prime the symbol $Art_{\infty,F/K}$ is in $\mathrm{Gal}(F/L)$ and is non-trivial if and only if F is totally complex.*

A field F satisfying these properties is said to be *correct for a, b and c*. Let $a, b, c \in \mathbb{Z}$ satisfying A) and B). We define the Redei symbol as

$$[a,b,c]_F := \begin{cases} \mathrm{Art}_{\mathfrak{c},F/K} & \text{if } c > 0 \\ \mathrm{Art}_{\infty,F/K} \cdot [a,b,-c]_F & \text{if } c < 0. \end{cases}$$

Lemma 2 *Let a, b, c as before and let F and F' be correct fields for a, b, c. Then $[a,b,c]_F = [a,b,c]_{F'}$.*

From now on we denote the Redei symbol simply as $[a,b,c]$. This symbol is easily seen to be symmetric in the first two entries, but the following law establishes a stronger fact:

Theorem 6 (Redei Reciprocity Law) *For every a, b, c satisfying the previous conditions, we have*

$$[a,b,c] = [b,a,c] = [a,c,b].$$

5 Applications to the study of the 8-rank

We now present how the Redei symbol is useful for the study of the 8-rank r_8. Recall that R is the map giving the value of the 4-rank r_4.

Theorem 7 *There exists a map $R_8 : KerR \to \mathbb{F}_2^{r_4}$ such that $r_8 = r_4 - rankR_8$. Moreover, let $(d_1^{(i)}, d_2^{(i)})_{i=1}^{r_4}$ such that the fields $\mathbb{Q}\left(\sqrt{d_1^{(i)}}, \sqrt{d_2^{(i)}}\right)$ generate the extension $\hat{L}/K$ of degree 2^{r_4} corresponding to $C/(C[2] \cap 2C)$. Then R_8 maps an ideal class $[\mathfrak{m}]$, with $\mathfrak{m}$ of norm m, to the r_4-tuple $([d_1^{(i)}, d_2^{(i)}, m])$.*

As a final application, the theory developed so far allows to provide a new proof for the following result:

Theorem 8 *Let $d \in \mathbb{Z}$ not a square. Then there exists a Galois extension $\Omega_8/\mathbb{Q}$ such that, if p_1 and p_2 are odd prime numbers that do not divide d and have the same Artin symbol in $\Omega_8/\mathbb{Q}$, then $C(\mathbb{Q}(\sqrt{dp_1}))$ and $C(\mathbb{Q}(\sqrt{dp_2}))$ have the same 2,4,8-rank.*

This statement was first conjectured by Cohn and Lagarias in [1] and proved by Stevenhagen in [7]. A simpler proof via the Redei symbols was given by Corsman [2] and corrected by Iadarola [4].

References

[1] H. Cohn and J. C. Lagarias. On the existence of fields governing the 2-invariants of the classgroup of $\mathbb{Q}(\sqrt{dp})$ as p varies. *Math. Comp.*, 41(164):711–730, 1983.

[2] J. Corsman. *Redei symbols and governing fields*. ProQuest LLC, Ann Arbor, MI, 2007. Thesis (Ph.D.)–McMaster University (Canada).

[3] C. F. Gauss. *Disquisitiones arithmeticae*. Translated into English by Arthur A. Clarke, S. J. Yale University Press, New Haven, Conn.-London, 1966.

[4] A. Iadarola. *On the 8-rank of quadratic class groups*. 2017. Thesis (Master)–Universiteit Leiden (Netherlands).

[5] L. Rédei. Arithmetischer Beweis des Satzes über die Anzahl der durch vier teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper. *J. Reine Angew. Math.*, 171:55–60, 1934.

[6] L. Rédei. Ein neues zahlentheoretisches Symbol mit Anwendungen auf die Theorie der quadratischen Zahlkörper. I. *J. Reine Angew. Math.*, 180:1–43, 1939.

[7] P. Stevenhagen. Ray class groups and governing fields. In *Théorie des nombres, Année 1988/89, Fasc. 1*, Publ. Math. Fac. Sci. Besançon, page 93. Univ. Franche-Comté, Besançon, 1989.

Francesco Battistoni
Dipartimento di Matematica
Universita degli Studi di Milano
Via Saldini 50
20133 Milano, Italy.
email: francesco.battistoni@unimi.it

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 4, *Number* 1, *March* 2019, *pages* 17-22

Christian Maire

Pro-p-extensions of number fields and relations

Written by Zouhair Boughadi

This note presents a summary of the talk of Christian Maire at the fourth mini symposium of the Roman number theory association based on a joint work with F. Hajir and R. Ramakrishna. The main results of the talk are a new record to the constant of Martinet and the answer to a question asked by Ihara. The construction of infinite unramified pro-p-extension of a number field plays a crucial role in the proof of these results.
Let G be a pro-p-group, we denote $h^i(G) = dim_{\mathbb{F}_p} H^i(G, \mathbb{F}_p)$, $d(G) = h^1(G)$, and $r(G) = h^2(G)$

Theorem 0.1 (Golod-Shafarevich) *Let G be a non trivial finite p-group. Then*

$$r(G) > \frac{d(G)^2}{4}.$$

For a number field K, let's denote by K' the maximal pro-p-extension of K which is unramified everywhere and $G = Gal(K'/K)$ its Galois group. We know that the group G is a finitely presented pro-p-group. Moreover, by class field theory, we know that $d(G)$ is exactly the p-rank of the class group of K. We also have bounds for the number of relations

of G, obtained by Koch and Shafarevich :

$$d(G) \leq r(G) \leq d(G) + r_2 + r_1 - 1 + \delta_{K,p},$$

where r_2 (resp. r_1) is the number of complex (resp. real) embeddings and $\delta_{K,p}$ is equal 1 or 0 depending on whether K contains or not the pth root of unity μ_p.

Theorem 0.2 *If $d(Cl_K) \geq 2 + 2\sqrt{r_2 + r_1 + \delta_{K,p}}$, then K'/K is infinite.*

Let G be a pro-p-group, and let

$$1 \longrightarrow R \longrightarrow F \longrightarrow G \longrightarrow 1$$

be a minimal presentation of G, then the pro-p-group F is a free group with $d(G)$ generators.
Let $\Lambda := \mathbb{F}_p[[F]]$ be the Iwasawa algebra of F and

$$I = ker(\Lambda \to \mathbb{F}_p)$$

be the augmentation ideal of Λ.
The depth $\omega(g)$ of an element g of $F \setminus \{1\}$ is defined as

$$\omega(g) = max\{n, g - 1 \in I^n\}.$$

The Zassenhaus filtration of F is given by

$$F_n = \{g \in F,\ \omega(g) \geq n\}.$$

It is well known that $R/R^p[F,R] \simeq H^2(G, \mathbb{F}_p)$. Let $(\rho_i)_i$ be a set of generators of $R/R^p[F,R]$, for $n \geq 1$ we set

$$r_n = |\{\rho_i,\ \omega(\rho_i) = n\}|.$$

Note that r_1 always equals zero because of the following isomorphism

$$G/G^p[G,G] \simeq F/F^p[F,F].$$

Theorem 0.3 (Vinberg, 1965) *If the series* $1 - d(G)t + \sum_n r_n t^n$ *has a zero for a given* $t \in [0, 1]$*, then the pro-p-group G is infinite.*

As an application, if one has no information on the relations, we take $r_2 = r(G)$ to obtain the Golod Shafarevich theorem. More generally if we suppose that $r_2 = \cdots = r_{k-1} = 0$ we get a refinement of Golod Shafarevich bound; namely, if G is finite then

$$r(G) > \frac{d(G)^k}{k^k}(k-1)^{k-1}.$$

A similar result was proven by Koch-Venkov and Schoof, when p is an odd prime and K a quadratic field. Then $r_2(G) = 0$, furthermore if $h^1(G) \leq 3$, K'/K is infinite. More generally Kisilevsky-Labute asserts that this result remains true when K is a CM field.
The main results of the talk can be viewed as further applications. We start with the new record of Martinet's constant. Let K be a number field and (r_1, r_2) its signature ($[K : \mathbb{Q}] = r_1 + 2r_2$). We define the root discriminant of K to be

$$Rd_K := |Disc_K|^{1/[K:\mathbb{Q}]},$$

where $Disc_K$ is the discrimant of K. For number fields with $[K : \mathbb{Q}] >> 0$ and by classical methods we have

$$Rd_K \geq A^t B^{1-t}$$

where $t = r_1/[K : \mathbb{Q}]$ denotes the type of K.
The constants A and B are still unknown, but lower bounds are given

	Minkowski	Odlyzko	Odlyzko (GRH)
$A \geq$	7.3	60.8	215.3
$B \geq$	5.8	22.3	44.7

Two upper bounds for the constants A and B are the constants of Martinet

$$\alpha(0,1) := \liminf_n \min\{Rd_K, [K : \mathbb{Q}] = 2n, K \text{totally imaginary}\}$$
$$\alpha(1,0) := \liminf_n \min\{Rd_K, [K : \mathbb{Q}] = n, K \text{totally real}\}$$

It is well known that we have

$$A \leq \alpha(1,0) \text{ and } B \leq \alpha(0,1).$$

On the other hand, upper bounds for $\alpha(.,.)$ occur using the discriminant formula and infinite unramified extensions. The first one was given by Jaques Martinet in 1978; he proved that the field $K = \mathbb{Q}(\sqrt{2}, \sqrt{-23}, \cos(2\pi/11))$ has an infinite unramified extension, and so

$$\alpha(0,1) \leq Rd_K \sim 92.4\cdots$$

	Martinet (1978)	Hajir-Maire (2002)
$\alpha(1,0) \leq$	$1058.6\cdots$	$954.3\cdots$
$\alpha(1,0) \leq$	$92.4\cdots$	$82.2\cdots$

The new record is given in this talk

$$\alpha(1,0) \leq 857.5\cdots \quad (1)$$
$$\alpha(0,1) \leq 78.5\cdots \quad (2)$$

This record is obtained by observing that the totally imaginary example of Hajir-Maire improving Martinet's record gives an infinite unramified extension with root discriminant less than 78.5. This extension is obtained by cutting the maximal unramified extension outside a prime ideal of norm equal to 9, by a fourth power of its generator of its inertia group.
The second application is the answer to Ihara's question. Given an infinite unramified extension L/K, denote by $\mathcal{S}(L/K)$ the set of prime ideals of K that decompose completely in L/K.

$$\sum_{\mathfrak{p}\in\mathcal{S}(L/K)} \frac{\log N(\mathfrak{p})}{\sqrt{\log N(\mathfrak{p})}} < \infty$$

Can $\mathcal{S}(L/K)$ be infinite?
An answer is the following

Theorem 0.4 (HMR, 2018) *Suppose that* $d(Cl_K) > 2+2\sqrt{r_1 + r_2 + 1}$. *Then there exists an infinite unramified pro-p-extension* L/K *for which* $\mathcal{S}(L/K)$ *is infinite.*

The last one is about p-rational fields. Let K_p be the maximal pro-p-extension of K unramified outside p. Class field theory gives a description of the abelianization of G_p

$$G_p/[G_p, G_p] \simeq \mathbb{Z}_p^{r_2+1+\delta_K}$$

where δ_K is the Leopoldt defect, conjecturally null (Leopoldt conjecture)

Definition 0.5 *When* G_p *is pro-p-free, the number field* K *is said p-rational.*

In 2016, Gras gave the following

Conjecture 1 *Every number field* K *is p-rational for all* $p \geq C(K)$.

Theorem 0.6 *Let* $K/\mathbb{Q}$ *be a totally imaginary extension of degree at least 12. Choose* $p > 2$ *such that:*

i) *p splits totally in* $K/\mathbb{Q}$*;*

ii) K *is p-rational.*

Then there exists a finite extension F/K *in* K_p/K *such that* $F^{ur,p}/F$ *is infinite.*

References

[1] F. Hajir, C. Maire and R. Ramakrishna, *Cutting towers of number fields*. *arXiv:1901.04354*, preprint 2018.

[2] F. Hajir and C. Maire, *Unramified Subextensions of Ray Class Field Towers*. *Journal of Algebra*, 249:528–543, 2002.

[3] J. Martinet, *Tours de corps de classes et estimations de discriminants*. *Inventiones math.*, 44:65–73, 1978.

[4] Y. Ihara, *How many primes decompose completely in an infinite unramified Galois extension of a global field ?*. *J. Math. Soc. Japan*, 35(4):693–709, 1983.

Zouhair Boughadi
department of mathematics and informatics
Moulay Ismail university
B.P. 11201 Zitoune Meknes
50070, Morocco.
email: z.boughadi@edu.umi.ac.ma

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 4, *Number* 1, *March* 2019, *pages* 23-33

Pietro Corvaja

A superficial viewpoint on certain Diophantine equations

Written by Abdelaziz El Habibi

Investigating solutions in integers of systems of algebraic equations is one of the main objects of Diophantine Geometry. Given polynomials $f_1(X_1, ..., X_N)$,...,$f_k(X_1, ..., X_N) \in \mathbb{Z}[X_1, ..., X_N]$, we consider the solutions $(x_1, ..., x_N) \in \mathbb{Z}^N$ or $\mathbb{Q}^N$ to the system

$$\begin{cases} f_1(x_1, ..., x_N) = 0 \\ \qquad \vdots \\ f_k(x_1, ..., x_N) = 0 \end{cases}$$

The complex solutions to the above system form an algebraic variety. We shall be especially interested in the case where such an algebraic variety is a surface. We shall see that many interesting open problems on Diophantine equations boil down to describing integral or rational points on algebraic surfaces; we shall then speak of *s*uperficial problems.

The Box problem and Euler bricks.

A first superficial problem about rational points is the so called the box problem: Does there exists a box whose sides, face diagonals and

space diagonal all have integral length ?
The equations corresponding to the box problem are the following:

$$\begin{cases} x_1^2 + x_2^2 = y_3^2 \\ x_2^2 + x_3^2 = y_1^2 \\ x_3^2 + x_1^2 = y_2^2 \\ x_1^2 + x_2^2 + x_3^2 = z^2 \end{cases} \tag{1}$$

Note that it is a system of homogenous equations. Viewing each solution as a point $(x_1 : x_2 : x_3 : y_1 : y_2 : y_3 : z)$ in the six-dimensional projective space, the system (1) defines an algebraic surface $\mathcal{S} \subset \mathbb{P}_6$. The points on this surface we are interested in are the rational points outside the 'trivial' curves where some coordinate vanishes.

The surface $\mathcal{S}$ is of general type: after Bombieri's Conjecture, it is believed that its rational points are not Zariski-dense. However, it is unkown whether it admits one single non-trivial rational point.

We could relax the conditions by omitting the requirement that the space diagonal of the box be rational. In other words, we are searching for triples of integers (x_1, x_2, x_3) such that any two of them belong to a Pytagorean triple. Such solids are common called Euler bricks. An example is given by the solution

$$(x_1 : x_2 : x_3 : y_1 : y_2 : y_3) = (44 : 117 : 240 : 267 : 244 : 125). \tag{2}$$

For this problem, the resulting surface is a (singular model of a) $K3$ surface; its rational points are Zariski-dense, as we shall now prove.

Let $\mathcal{X}$ be this surface, which is then defined in the five-dimensional projective space by the system of equations

$$\begin{cases} x_1^2 + x_2^2 = y_3^2 \\ x_2^2 + x_3^2 = y_1^2 \\ x_3^2 + x_1^2 = y_2^2 \end{cases} \tag{3}$$

First note that its only singularities are the isolated points

$$(0 : 0 : 1 : 1 : 1 : 0), (0 : 1 : 0 : 1 : 0 : 1), (1 : 0 : 0 : 0 : 1 : 1).$$

Letting C be the (plane) conic of equation $x_1^2 + x_2^2 = y_3^2$, the projection $\pi : \mathcal{X} \dashrightarrow C$ (undefined only on the first singular point) sending

$$\mathcal{X} \ni (x_1 : x_2 : x_3 : y_1 : y_2 : y_3) \mapsto (x_1 : x_2 : y_3)$$

admits for generic fibers the curves of genus 1 of equation

$$\begin{cases} x_2^2 + x_3^2 = y_1^2 \\ x_3^2 + x_1^2 = y_2^2 \end{cases} \tag{4}$$

These curves are irreducible and smooth whenever $x_1 x_2 y_3 \neq 0$. For each point $p = (x_1 : x_2 : y_3)$ on the conic C, the fiber $E_p = \pi^{-1}(p)$ admits a distinguished point O_p, namely the point

$$O_p = (x_1 : x_2 : 0 : x_2 : x_1 : y_3).$$

Taking the point O_p for the origin, a group law on E_p is well defined, so that E_p becomes an elliptic curve. Note the presence of three other rational points, namely $(x_1 : x_2 : 0 : -x_2 : x_1 : y_3), (x_1 : x_2 : 0 : x_2 : -x_1 : y_3)$ and $(x_1 : x_2 : 0 : -x_2 : -x_1 : y_3)$; these points are torsion points for the group law.

Consider now the following rational curve $\mathcal{D}$ on the surface, parametrized as follows: for every point $(a : b : c)$ in the conic $\mathcal{D}' : a^2 + b^2 = c^2$, put

$$\begin{cases} x_1 = a(4b^2 - c^2) \\ x_2 = b(4a^2 - c^2) \\ x_3 = 4abc \\ y_1 = b(4a^2 + c^2) \\ y_2 = a(4b^2 + c^2) \\ y_3 = c^3 \end{cases}$$

This curve, which gives rise to an infinite family of Euler bricks, was found by Saunders already in 1740.

Note that the map

$$(a : b : c) \mapsto \varphi(a : b : c) = (x_1 : x_2 : y_3) \\ = (a(4b^2 - c^2) : b(4a^2 - c^2) : c^3) \in C$$

is a degree three covering of the conic C by the isomorphic conic $\mathcal{D}'$ (which is also isomorphic to the rational curve $\mathcal{D} \subset \mathcal{X} \subset \mathbb{P}_5$). Now, each fiber E_p of the already described elliptic fibration intersects the conic in three points; if the point $p = (x_1 : x_2 : y_3) \in C$ comes from a rational point of $\mathcal{D}$ via the map φ described above, one of these points on E_p is rational. We then obtain that infinitely many elliptic curves E_p adimt an extra rational point, in addition to the point O_p and the three mentioned torsion points. This new rational point is in general of infinite order (as we shall see in a moment), so infinitely many fibers E_p contain infinitely many rational points. This shows that the rational points on the surface are Zariski-dense.

Geometrically, the points on E_p, coming from the curve $\mathcal{D}'$ can be described as follows: consider the two projections $\pi : \mathcal{X} \to C$ and $\varphi : \mathcal{D}' \to C$; the correponding fiber product gives rise to a new surface $\mathcal{Y}$ endowed with a finite map $\psi : \mathcal{Y} \to \mathcal{X}$ and an elliptic fibration $\mathcal{Y} \to \mathcal{D}'$. This elliptic fibration admits a section $\sigma : \mathcal{D} \to \mathcal{Y}$. The image of a point $q = (a : b : c) \in \mathcal{D}'$ is a point $\sigma(q) \in \mathcal{Y}$ such that

$$\pi(\psi(\sigma(q))) = \varphi(q).$$

It remains to show that infinitely many points $\sigma(q)$, for q a rational point on $\mathcal{D}'$ are non-torsion. By well-known result, this amounts to prove that σ is not identically torsion, which is equivalent to saying that for at least one point q, $\sigma(q)$ is non-torsion. We leave to the reader the task of verifying that for $q = (3 : 4 : 5)$ (the simples Pytagorean triple!), the image of $\sigma(q)$ on $\mathcal{X}$, namely the point appearing in (2), is non-torsion on the corresponding elliptic curve.

Let us come back to our original surface $\mathcal{S}$ whose (non-trivial) rational points correspond to the (possible) solutions to the original

Box problem. As we said, it is a surface of general type, and we do not know whether it contains any non-trivial rational point, and not even whether its rational points might form a infinite set, or a Zariski-dense set.

We conjecture the finiteness of its rational points, but we can prove unconditionally only the result below, for which we need the following definition: Let $\mathcal{R}$ be the radical function, associating to a positive real number the product of its prime divisors. Put

$$\mathcal{R}(x_1, x_2, x_3) := \mathcal{R}(\gcd(x_1, x_2).\gcd(x_2, x_3).\gcd(x_3, x_1)).$$

Then we can prove

Theorem 0.1 *For any (possible) infinite sequences in $\mathcal{S}(\mathbb{Q})$,*

$$\mathcal{R}(x_1, x_2, x_3) \longrightarrow \infty.$$

In the above statement, it is meant that the rational point $(x_1 : x_2 : x_3 : y_1 : y_2 : y_3 : z)$ is written with coprime integral coordinates. The Theorem impliess that one cannot take the coordinates to be *pairwise* coprime. Actually, it is easy to see that the prime 2 must divide at least one of the $\gcd(x_1, x_2)$, $\gcd(x_2, x_3)$, $\gcd(x_3, x_1)$; the theorem states moreover that infinitely many other primes must appear in the corresponding gcd, for every sequence of solutions.

Proof. The proof consists of an application of the Chevalley-Weil theorem; namely, we construct a finite covering $\mathcal{Z} \to \mathcal{X}$ to which the rational points of $\mathcal{X}$ can be lifted to points defined over a number field which only depends on $\mathcal{R}(x_1, x_2, x_3)$. Then apply Falting's theorem to the surface $\mathcal{Z}$, which turns out to be the product of two curves.

Suppose by contradiction that $\mathcal{R}(x_1, x_2, x_3)$ is bounded on an infinite sequence of rational points. Then there exists a finite set of primes S such that all the rational points in such a sequence never reduce to one singular point of the surface $\mathcal{S}$ modulo any prime outside the set S. In another language, they are S-integers with respect to the subvariety formed by the singular locus of the surface (note that after

desingularizing, such a locus becomes a finite union of irreducible curves).

For each pair of indices $1 \leq h < k \leq 3$, one of the equations (1) defining S implies that for each rational point of the surface the quantity $x_h^2 + x_k^2$ is a perfect square. Now, in the ring $\mathbb{Z}[i]$ the above expression factors as

$$x_h^2 + x_k^2 = (x_h + ix_k)(x_h - ix_k).$$

If the product is a square and the factors are coprime, each factor is a square (at least up to multiplication by a unit in the ring $\mathbb{Z}[i]$): this is the basic principle behind the so called Chevalley-Weil theorem. We are supposing that the two factors can have common prime divisors only outside the set S (more precisely, outside the set of primes in $Z[i]$ lying above one prime of S). Hence, there exists a finite extension κ of $\mathbb{Q}(i)$ such that each factor $x_h + ix_k$ is a square in the ring of integers of such a number field.

We then obtain that the rational points on $\mathcal{S}$ lift to κ- rational points on the variety defined by the system of equations

$$\begin{cases} x_1 + ix_2 = u_3^2 \\ x_1 - ix_2 = v_3^2 \\ x_2 + ix_3 = u_1^2 \\ x_2 - ix_3 = v_1^2 \\ x_3 + ix_1 = u_2^2 \\ x_3 - ix_1 = v_2^2 \\ x_1^2 + x_2^2 + x_3^2 = z^2 \end{cases} \tag{5}$$

This is the equation of another surface $\mathcal{Z}$ covering by a finite map (of degree 8) our surface $\mathcal{S}$. We claim that Z is isomorphic to the product of a genus 5 curve with itself. Then, by Faltings' theorem, the surface $\mathcal{Z}$ contains only finitely many rational point on any given number field, concluding the argument.

Let us prove our claim. Looking first at the last equation in (5), we see that the surface $\mathcal{Z}$ is a degree 64 cover of a smooth quadric,

which is isomorphic, over the complex (and even over the number field $\mathbb{Q}(i)$) to the square of the projective line. The covering $\mathcal{Z} \to \mathbb{P}_1 \times \mathbb{P}_1$ ramifies only over the curves of equation $x_h \pm i x_h = 0$, which are pairs of lines. Removing their pre-images from the surface $\mathcal{Z}$, and calling $\mathcal{Z}^*$ the corresponding open surface, we obtain an unramified cover $\mathcal{Z}^* \to (\mathbb{P}_1 \setminus (F))^2$, where F is a finite set of cardinality 6. Now, every unramified covering of a product is covered by a product of unramified covers; in our case, we have an abelian unramified cover of $\mathbb{P}_1 \setminus F$, of type $(2, 2, 2)$, obtained as a fibred product of three degree 2 covers each ramified over two points; the genus of the resulting curve turns out to be five, so Faltings' theorem provides finiteness.

The Markov equation

The equation

$$x^2 + y^2 + z^2 = 3xyz,$$

is called the Markov equation. It is the equation of a singular affine surface $\mathcal{M}$ in three-space. Markov triples are defined as the solutions (x, y, z), with x, y, z positive integers, to Markov's equation; we call any positive integer x which appears in a Markov triple a Markov number, and we call any pair (x, y) such that for some integer z the triple (x, y, z) is a Markov triple a *Markov pair*. A question about the arithmetic nature of Markov numbers is the following: does the greatest prime factor of a Markov number tend to infinity? If not, there would exist infinitely many Markov numbers which are S-units for a fixed finite set of places S; it is still an open problem.

Recalling that $\mathcal{R}(.)$ denotes the radical of an integer the problem boils down to understanding whther $\mathcal{R}(x)$ must tend to infinity on every infinite sequence of Markov numbers. We do not know the answer, but dispose of the weaker result:

Theorem 0.2 (Theorem 1 in [2]) *For every infinite sequences of Markov pairs, we have*

$$\mathcal{R}(xy) \longrightarrow \infty.$$

Idea of the proof. The proof uses the subspace theorem after reducing to a problem about itegral points. Suppose that $\mathcal{R}(xy)$ is bounded on an infinite sequence. Then for some fixed integer R, the Markov equation has infinitely many solutions (x, y, z) where $z \in \mathbb{Z}$ and x, y are units in the ring $\mathbb{Z}[1/R]$.

Note that once x, y are fixed integers, the Markov equation in z can be solved whenever the quantity

$$9x^2y^2 - 4(x^2 + y^2)$$

is a perfect square. Putting $x^2 = u, y^2 = v$ we obtain the quadratic equation

$$9uv - 4u - 4v = \delta^2,$$

which in homogeneous form becomes

$$9uv - 4uw - 4vw = \delta^2. \tag{6}$$

This is the equation of a smooth quadric surface in $\mathbb{P}_3$. The condition that u, v, δ are integers amounts to an integrality condition on the rational point $(u : v : w : \delta)$ with respect to the divisor $w = 0$ on the surface (see [1], chap. 1 for a precise definition of the notion of integrality with respect to a divisor). Similarly, requiring that x, y, so u, v, are R-units amounts to the integrality with respect to the divisor $uv = 0$. We must then consider the complement of the divisor D of equation $uvw = 0$ on the smooth quadric defined by (6). This divisor is the sum of three smooth conics; identifying the surface with the product $\mathbb{P}_1 \times \mathbb{P}_1$, the divisor D has bidegree $(3, 3)$; note that any canonical divisor K on $\mathbb{P}_1 \times \mathbb{P}_1$ had bidegree $(-2 - 2)$, so the sum $D + K$ is ample. According to Vojta's Conjecture, the D-integral points on the surface should not be Zariski-dense. Although we are not able to prove Vojta's Conjecture for this class of open surfaces, an application of the Subspace Theorem as described in [2] proves the desired result when z is supposed to be an integer in the classical sense, not merely an R-integer.

Elliptic curves over $\mathbb{Q}$

Let E be an elliptic curve over $\mathbb{Q}$ be defined by a Weierstrass equation:

$$y^2 = x^3 + ax + b,$$

where $a, b \in \mathbb{Z}$ are integers with $4a^3 - 27b^2 \neq 0$. For a rational solution $P = (x_1, x_2) \in \mathbb{Q}^2$ of the above equation, one can write the rational numbers x, y in a unique way as

$$(x, y) = (\tfrac{u}{d^2}, \tfrac{v}{d^3}),$$

for coprime integers u, v and $d > 0$. We define the denominator of $P = (x, y)$ to be the integer $d(P) = d$.

The following Conjecture, which is a consequence of Vojta's conjecture on surfaces, gives a criterion for identifying elliptic curves by studying the denominators of their rational points.

Conjecture 1 *Let E_1 and E_2 be two elliptic curves over $\mathbb{Q}$ with infinitely many rational points. Suppose there exist infinitely many pairs $(P_1, P_2) \in E_1(\mathbb{Q}) \times E_2(\mathbb{Q})$ for which*

$$(*) \quad d(P_1) = d(P_2).$$

Then E_1 and E_2 are isomorphic, and after identifying $E_1 \simeq E_2$, for all but finitely many solutions (P_1, P_2) to $(*)$, $P_1 = \pm P_2$.

Although the problem is formulated in terms of rational points on curves, it turns out to be in fact a problem on integral points on surfaces, as we shall see in a moment. We first recall a related result of Corrles-Rodriganez and Schoof from [4]:

Proposition 0.3 *Let $P_1 \in E_1(\mathbb{Q})$ and $P_2 \in E_2(\mathbb{Q})$ of infinite order; if*

$$\mathcal{R}(d(nP_1))|\mathcal{R}(d(nP_2))$$

for all $n \in \mathbb{N}$, then E_1 and E_2 are isogenous over $\mathbb{Q}$.

A second conclusion asserts that for all but finitely many solutions, P_2 is the image of P_1 by a suitable isogeny $E_1 \to E_2$.

The next theorem is a particular case of the above Conjecture; it is a curious application of a general result of Vojta on subvarieties of semi-abelian varieties.

Theorem 0.4 *Let E_1 and E_2 be two elliptic curves defined over $\mathbb{Q}$. Suppose that for infinitely many pairs $(P_1, P_2) \in E_1(\mathbb{Q}) \times E_2(\mathbb{Q})$,*

$$d(P_1) = d(P_2) \quad \text{and} \quad d(2P_1) = d(2P_2). \tag{7}$$

Then E_1 is isomorphic to E_2 and, after identifying E_1 with E_2, for all but finitely many such pairs, $P_1 = \pm P_2$.

This is Theorem 3.32 in [3]. The proof consists in viewing the solutions to (7) as integral points on the complement of a certain divisors in a blow-up of the surface $E_1 \times E_2$. Such an open surface can be embedded into a semi-abelian variety, namely the product of the multiplicative group by the abelian surface $E - 1 \times E_2$, and then the mentioned result by Vojta applies.

References

[1] P. Corvaja, *Integral Points on Algebraic Varieties. An introduction to Diophantine Geometry. Institute of Mathematical Sciences Lecture Notes, Hindustan Book Agency, New Delhi*, 2016.

[2] P. Corvaja and U. Zannier *On the greatest prime factor of Markov pairs*, *Rendiconti del Seminario Mat. della Università di Padova*, 116:253–260, 2006.

[3] P. Corvaja and U. Zannier *Applications of Diophantine Approximation to Integral Points and Transcendence*, *Cambridge Tracts in Mathematics* 212, Cambridge University Press, 2018.

[4] C. Corrales and R. Schoof *The support problem and its elliptic analogue*, *J. Number Theory*, 64:276–290, 1997.

[5] J.H. Silverman, J. Tate, *Rational points on elliptic curves*, *Second edition, Springer*, 2015.

Abdelaziz EL Habibi
Department of Mathematics and Informatics
Mohammed First University
BV Mohammed VI BP 717 60000 Oujda, Morocco.
email: abdelaziz.elhabibi92@gmail.com

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 4, *Number* 1, *March* 2019, *pages* 35-42

Evelina Viada

Rational Points on Curves

Written by Manoj Gyawali

1 Introduction

One of the oldest problem in Diophantine geometry is that of the complete determination of the set of rational (or k-rational) points, of a given algebraic curve defined over the rational numbers (or more generally over a number fields). Clearly a rational curve (i.e. a curve of genus zero) defined over a number field if it has one rational point it has infinitely many. For algebraic curves of genus one with one specified rational point (i.e. elliptic curves), we have the following, by now classical, result of Mordell and Weil.

Theorem 1.1 (Mordell-Weil Theorem) *Let E be an elliptic curve defined over a number field k. Then the set $E(k)$ of k-rational points of E is a finitely generated abelian group.*

The next case is that of algebraic curves of genus greater than 1. From now on, by a curve C we mean an algebraic curve defined over the algebraic numbers $\overline{\mathbb{Q}}$ and for k a number field. We denote the k-rational points of C by $C(k)$. Mordell conjectured in 1922 that a curve of genus at least 2 has only finitely many points over any number field. This was proven by Faltings in 1983, see [4]

Theorem 1.2 (Faltings) *Let C be a curve defined over a number field k. Suppose the genus of C is at least 2, then $C(k)$ is finite.*

Unfortunately Falting's theorem is not effective, which means in particular that there is no effective bound for the height of the points in $C(k)$. The aim of this seminar is to present an effective bound on the height of the k-rational points on some families of curves, which in turn led to the complete determination of the set of rational points for the curves of the families in question.

2 Torsion and finiteness

Let A be an abelian variety, Γ a finitely generated subgroup and X an irreducible subvariety of A. In this section we dwell briefly on the following problem: If X has a large (i.e. Zariski dense) intersection with Γ what can be said about X? It all started with the celebrated Manin-Mumford conjecture (raised independently by Manin and Mumford), proved by Raynaud [9].

Theorem 2.1 (Raynaud) *Let A be an abelian variety and Tor_A its torsion subgroup. Let $C \subset A$ be a curve of genus ≥ 2. Then, $C \cap Tor_A$ is finite.*

Both Mordell conjecture and Manin-Mumford conjecture are special cases of the Mordell-Lang conjecture, put forward by Serge Lang in 1965 [7]. The Mordell-Lang conjecture for curves can be stated as follows:

Mordell-Lang Conjecture *Let C be an irreducible curve of a (semi) abelian variety A defined over a number field k. Let Γ be a finitely generated subgroup of $A(k)$ and Γ' a subgroup of the divisible hull of Γ (i.e. for each $x \in \Gamma'$ there exists a non-zero integer n such that $nx \in \Gamma$). If C is not a translate of a (semi) abelian subvariety of A, then $C(k) \cap \Gamma'$ is finite.*

The general statement of the Mordell-Lang conjecture for varieties was proven by McQuillan in 1995 ([8]) building on the break through result of Faltings [5], on the result of Hindry [6] and using a result of Vojta [12]. For more information about this topic we refer the reader to [10]

Next, along this thread of thought, comes the theme of unlike intersections initiated by Bombieri, Masser and Zannier in [1]. In this setting one replaces the set of "special points" (i.e. Γ') with a set of special subvarieties (i.e. algebraic subgroups of A). In order to state the two most relevant conjectures in this setting we need some definitions.

Definition 2.1 A variety $X \subset A$ is called a *torsion variety* (respectively a *translate*) if it is a finite union of translates of algebraic subgroups of A by torsion points (respectively by points).

Definition 2.2 An irreducible variety $X \subset A$ is called *transverse* (respectively *weak-transverse*) if it is not contained in any proper translate (respectively any proper torsion variety).

The Torsion Anomalous Conjecture, which we state below for the case of a weak-transverse curve, has been open for several years:

Torsion Anomalous Conjecture *Let C be a weak-transverse curve in A. Then the set*

$$C \bigcap \left(\bigcup_{\substack{B \text{ algebraic subgroup} \\ \dim B \leq \dim A - 2}} B \right)$$

is finite.

In the above mentioned seminal paper of Bombieri, Masser and Zannier, there is a proof of the Torsion Anomalous Conjecture for transverse curves in an algebraic torus. Their proof is based on the following two statements: (here $\mathcal{B}_2$ denotes the union of the algebraic subgroups of codimension at least 2)

- The points of $C \cap \mathcal{B}_2$ have bounded height.
- The points of $C \cap \mathcal{B}_2$ have bounded degree.

For if the two above conditions are satisfied then the classical Northcott theorem yields the finiteness of $C \cap \mathcal{B}_2$. A central aspect of their proof is that it is effective. This is relevant to find bounds, and even better effective bounds for the height of points in $C \cap \mathcal{B}_2$.

In the course of their investigations around the Torsion Anomalous Conjecture, Checcoli, Veneziano e Viada proved, in [2] a very interesting bound on the height of points of curves contained in a power of a non-CM elliptic curves which we reproduce below. This result improves drastically on some previous bounds proved by the same authors in [3]. The bound proven in [3] is a consequence of a more classical approximation used in connection with the Torsion Anomalous Conjecture, we refer the reader to [3, Theorem 1.1 and Theorem 1.3], see also [11]. The bound in [2] is obtained by introducing new key elements in the proof. It has to be noted that this better bounds are crucial for practical applications, two instances of which will be presented in the final section. In order to state the theorem we need to recall a few definitions regarding heights. Let E be an elliptic curve given in $\mathbb{P}^2$ by the Weierstrass equation $y^2 = x^3 + Ax + B$ with A, B integral. We let $\hat{h}$ be the Néron-Tate height on E^N determined via the Segre embedding. Given a curve $C \subset E^N$ we denote by $h(C)$ the normalised height of C. Finally we denote by $h_W(\alpha)$ the Weil height of an algebraic number α. The following is a simplified version of the main theorem of [2].

Theorem 2.2 *Let E be a non-CM elliptic curve of $\mathbb{Q}$-rank 1. Let $C \subset E^N$ be an irreducibel curve of genus at least 2. Let $C_1 = 145$ and $c_1 = c_1(E) = 2h_W(A) + 2h_W(B) + 4$ with A and B the coefficients of the Weierstrass form. Then $P \in C(\mathbb{Q})$ has height bounded*

$$\hat{h}(P) \leq 4 \cdot 3^{N-2} N! \deg C (C_1 h(C)(\deg C) + 4C_1 c_2 (\deg C)^2 + 2c_1),$$

moreover if $N = 2$

$$\hat{h}(P) \leq C_1 \cdot h(C) deg\, C + 4C_1 c_1 (deg\, C)^2 + 4c_1.$$

If one specialises to a more particular case better bounds can be achieved:

Corollary 2.3 *Suppose* $(x_1, y_1) \times (x_2, y_2)$ *be the affine coordinates of* $E^2 \subseteq \mathbb{P}^2 \times \mathbb{P}^2$ *with* E *defined over* $\mathbb{Q}$. *Let* C *be the curve given in* E^2 *defined by the additional equation* $p(x_1) = y_2$, *with* $p(X) \in k[X]$ *a non-constant polynomial of degree* n. *Then* C *is irreducible and for* $P \in C(k)$ *we have*

$$\hat{h}(P) \leq 2595(h_W(p) + log n + 4c_1)(2n + 3)^2 + 4c_1$$

where $h_W(p) = h_W(1 : p_0 : \ldots : p_n)$ *is the Weil height of the coefficients of* $p(x)$ *and* $c_1 = 2log(3 + |A| + |B|) + 4$

3 Explicit examples

Consider the elliptic curve E defined by the Weierstrass equation

$$y^2 = x^3 + x - 1.$$

In the cartesian product $E \times E \subset \mathbb{P}^2 \times \mathbb{P}^2$ we use affine coordinates $(x_1,\ y_1)$ (respectively (x_2, y_2) on the first factor (respectively the second factor). Next we consider the $\{C_n\}$ family of curves in $E \times E$ given by the additional equation $x_1^n = y^2$. It turns out that the genus $g(C_n) = 4n + 2$ and C_n is irreducible for all n. As consequence of our main theorem we obtain a sharp bound for the height of the points on $C_n(\mathbb{Q})$. Moreover for n large, the points of $C_n(\mathbb{Q})$ will be integral. The bound on the height are so sharp that one can implement in SAGE an exhaustive search. Thus we obtain that

Theorem 3.1 *For all* $n \geq 1$ *the affine rational points of* C_n *are*

$$C_n(\mathbb{Q}) = \{(1,\ \pm 1) \times (1,\ 1)\}$$

Also the next example regards a family of curves, denoted by $\{\mathcal{D}_n\}$, lying in $E^2 = E \times E$. This time the additional equation defining the family of curves is $\Phi_n(x_1) = y_2$ where $\Phi_n(X)$ is the n-th cyclotomic polynomial. It can be shown that the curves $\mathcal{D}_n$ have increasing genus and are irreducible. Moreover, consider the following non-CM elliptic curves.

$$
\begin{aligned}
E_1 &: y^2 = x^3 - 26811x - 7320618,\\
E_2 &: y^2 = x^3 - 675243x - 213578568,\\
E_3 &: y^2 = x^3 - 110038419x + 12067837188462,\\
E_4 &: y^2 = x^3 - 2581990371x - 50433763600098.
\end{aligned}
$$

These elliptic curves have $\mathbb{Q}$ rank 1. For this family the characterisation of rational points is as follows:

Theorem 3.2 *For $i = 1, 2, 3, 4$ the curves $\mathcal{D}_n \subseteq E_i \times E_i$, there are no rational points other than the point at infinity. And for the curves $\mathcal{D}_n \subseteq E \times E$ we have the following affine rational points:*

$\mathcal{D}_1(\mathbb{Q}) = \{(2, \pm 3) \times (1, 1)\}$; $\mathcal{D}_2(\mathbb{Q}) = \{(2, \pm 3) \times (2, 3)\}$;

$\mathcal{D}_{3^k}(\mathbb{Q}) = \{(1, \pm 1) \times (2, 3)\}$; $\mathcal{D}_{47^k}(\mathbb{Q}) = \{(1, \pm 1) \times (13, 47)\}$;

$\mathcal{D}_{p^k}(\mathbb{Q}) = \varnothing$, *for* $p \neq 3, 47$ *and if* $p = 2$, $k > 1$;

$\mathcal{D}_6(\mathbb{Q}) = \{(1, \pm 1) \times (1, 1)\} \cup \{(2, \pm 3) \times (2, 3)\}$;

$\mathcal{D}_n(\mathbb{Q}) = \{(1, \pm 1) \times (1, 1)\}$ *if n has at least two distinct prime factors.*

Many other examples can be produced using the same techniques.

References

[1] E Bombieri, D. Masser and U. Zannier, *Intersecting a curve with algebraic sub- groups of multiplicative groups*, Internat. Math. Res. Notices, no. 20 (1999), 1119-1140.

[2] S. Checcoli, F. Veneziano and E. Viada, *The explicit Mordell Conjecture for families of curves (with an appendix by M. Stoll)*, preprint arXiv:1602.04097

[3] S. Checcoli, F. Veneziano and E. Viada, *On the explicit Torsion Anomalous Conjecture*, Journal: Trans. Amer. Math. Soc. 369(2017), 6465-6491.

[4] G.Faltings, *Endlichkeitssätze für ablsche Varietäten über Zahalkörpern*, Invent. Math, 73(1983),no.3, 349-366.

[5] G.Faltings, *The general case of S. Lang's Conjecture*, Barsotti Symposism in Algebraic Geometry (Abano Terme, 1991)Academic Press,San Diego,CA, 15(1994), 175-182.

[6] M.Hindry, *Autour d'une conjecture de Serge Lang*, Invent. Math, 96(1998), 575-603.

[7] S. Lang, *Division points on curves*, Ann. Mat. Pura Appl. (4) 70, 1965, 229-234.

[8] M. McQuillan, *Division Points on semi-abelian varieties*, Invent. Math.120(1995), no. 1, 143-159.

[9] M. Raynaud, *Sous-variete abelenne et points de torsion*, In Arithmetic and Geometry, vol.1,Birkhäuser (1983), 327-352.

[10] Pavlos Tzermos *The Manin-Mumford conjecture: a brief survey*, Bulletin of the London Mathematical Society Vol. 32, Issue 6 (2000), 641-652,

[11] E. Viada, *Explicit height bounds and the effective Mordell-Lang Conjecture*, Proceeding of the Third Italian Number Theory Meeting, Pisa, September 21-25, 2015, Riv. Mat. Univ. Parma, 7 (2016).

[12] P. Vojta, *Integral points on subvarieties of semiabelian varieties*, Invent. Math 126(1996),no. 1,133-181.

Manoj Gyawali
Department of Mathematics and Physics
Roma Tre University
Email: manoj.gyawali@ncit.edu.np

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 4, *Number* 1, *March* 2019, *pages* 43-47

Christophe Ritzenthaler

Primes of bad reduction of CM curves of genus 3

Written by Angelo Iadarola

1 Introduction

Let K be a discrete local field with valuation v, O its valuation ring, $k = O/\langle\pi\rangle$ its residue field, which we assume to have characteristic different from $2, 3, 5, 7$. In the following, we will be allowed to freely work on finite extensions of K, and we will say "after a finite extension of K". When F is an integral polynomial describing a plane curve, we denote by $\bar{F}$ its reduction modulo π.

Given a genus 3 non-hyperelliptic curve C/K, we want to determine the reduction type of its stable model C/O, possibly after a finite extension of K. In other words, we want to distinguish between

- C has *hyperelliptic reduction* if the reduction of its stable model $C \otimes k$ is a hyperelliptic curve of genus 3.
- C has *non-hyperelliptic reduction* if the reduction of its stable model $C \otimes k$ is a non-hyperelliptic curve of genus 3.
- C has *bad reduction* if the reduction of its stable model $C \otimes k$ is not a (smooth) curve of genus 3.

Example 1.1 *Let's consider the Klein quartic C over $\mathbb{Q}$, defined by the equation $x^3y + y^3z + z^3x = 0$. It is a smooth plane quartic (non-hyperelliptic) of genus 3. Its reduction is non-singular for every prime different from 7, in which case it is singular, irreducible and has 3 points.*
By changing coordinates, we can write the curve C_1, defined over $\mathbb{Q}(\sqrt{-7})$ and isomorphic to C, given by the equation

$$(x^2 + y^2 + z^2)^2 + \frac{\sqrt{-7} + 7}{2}(x^2y^2 + y^2z^2 + z^2x^2) = 0. \qquad (1)$$

When reducing modulo 7, we get the equation

$$(x^2 + y^2 + z^2)^2 = 0$$

which represents an hyperelliptic curve.

More generally, the main result concerning the relations between plane quartics and hyperelliptic genus 3 curves is the following, which can be found in [1].

Proposition 1.2 *Let $s > 0$ be an integer, $G \in O[x, y, z]$ a primitive quartic form and $Q \in O[x, y, z]$ a primitive quadratic form. Assume that $\bar{Q}$ is irreducible and $\bar{Q} = 0$ intersects $\bar{G} = 0$ transversely in 8 distinct $\bar{k}$-points.*
Then the smooth quartic $C/K : Q^2 + \pi^{2s}G = 0$ has hyperelliptic reduction.

For the sake of brevity, we can gather the hypothesis of the previous statement in the following definition.

Definition 1.3 *Given a smooth plane quartic C/K, if we can find a new curve K-isomorphic to C satisfying the hypothesis of the Proposition, we say that C admits a good toggle model.*

By explicit calculation, we can see that, indeed, the Klein quartic admits a good toggle model given precisely by (1), taking $Q = x^2 + y^2 + z^2$, $\pi = \frac{\sqrt{-7}+7}{2}$, $G = x^2y^2 + y^2z^2 + z^2x^2$ and $s = \frac{1}{2}$.

A first new result by the speaker and his coauthors is proving that the converse Proposition 1.2 holds [3, Theorem 2.8, 2.9].

Theorem 1.4 (Lercier, Liu, Lorenzo García, R.) *Let C/K be a smooth plane quartic. Then C has hyperelliptic reduction if and only if C admits a good toggle model over K.*

Further new results are characterizations for having (non-)hyperelliptic reduction, based on a set of invariants of the curve, the Dixmier invariants, which we will discuss in the following section.

2 Dixmier invariants and further results

Let's start by fixing the notation that we will use throughout this section. Given an n-tuple $\underline{d} = (d_1, \ldots, d_n) \in \mathbb{Z}_{>0}^{n+1}$, we denote by $\mathbb{P}^{\underline{d}}(K)$ the n-dimensional weighted projective space with weights given by the vector $\underline{d}$. Given a point $\underline{x} = (x_0, \ldots, x_n) \in \mathbb{P}^{\underline{d}}(K)$, possibly after a finite extension of K, we can always find a representative in $\mathbb{P}^{\underline{d}}(O)$ such that one of the coordinates has valuation 0; we call such a representative a *minimal representative* and denote it $\underline{x}^{\min}$. A priori, for a given $\underline{x}$, there are several different minimal representatives, but they all differ by the action of a unity, so, component-wise, they have the same valuation which we call the *normalized valuation with respect to* $\underline{x}$ of x_i and denote $v_{\underline{x}}(x_i)$.

In [2] Dixmier found 7 homogeneous polynomial invariants for the equivalence of ternary quartic forms under the action of $SL_3(\mathbb{C})$, which he called I_3, I_6, I_9, I_{12}, I_{15}, I_{18} and I_{27}, the indices being the degree of the polynomials. Moreover, he proved that they form a *homogeneous set of parameters*, from now on just HSOP, which means that all the invariants are equal to 0 for a quartic form in $\mathbb{C}[x_1, x_2, x_3]$ if and only if these 7 are. We call $\underline{DO}$ the 7-tuple made of these invariants and

we define $\underline{DO}(F)$ as the point of the weighted projective space, with weights given by the indices of the invariants, having as coordinates the evaluation of the invariants at the given ternary quartic form F, unless all the invariants are equal to 0, in which case, of course, we do not get a projective point. Finally, we denote $v_{DO}(I_\bullet(F))$ the normalized valuation with respect to $\underline{DO}(F)$.
Naturally, we can generalize this notation to any tuple of polynomial invariants $\underline{I}$ of any length, so we can now state the first result [3, Theorem 3.14]

Theorem 2.1 (Lercier, Liu, Lorenzo García, R.) *Let $\underline{I}$ be a tuple of invariants, C/K a smooth quartic curve defined by the ternary form $F = 0$. If $\underline{I}$ contains a HSOP over K and k, then C has non-hyperelliptic reduction if and only if $v_I(I_{27}(F)) = 0$.*

Finally the speaker and his coauthors found a new set of explicit invariants $\underline{\iota}$ in [3, Proposition 4.6] which let us give the final result [3, Theorem 1.6]

Theorem 2.2 (Lercier, Liu, Lorenzo García, R.) *There exist 2 sets of invariants, $\underline{DO}$, $\underline{\iota}$ such that a smooth quartic curve C/K defined by the ternary form $F = 0$ has hyperelliptic reduction if*

- $v_{DO}(I_3(F)) = 0$,
- $v_{DO}(I_{27}(F)) = 0$,
- $v_\iota(I_3(F)^5 I_{27}(F)) = 0$.

References

[1] C. H. Clemens, *A scrapbook of complex curve theory*. Plenum Press, New York-London, 1980. The University Series in Mathematics.

[2] J. Dixmier, *On the projective invariants of quartic plane curves*. Adv. in Math., 64:279–304, 1987.

[3] R. Lercier, Q. Liu, E. Lorenzo García, C. Ritzenthaler, *Reduction type of smooth quartics*. To appear.

Angelo Iadarola
Laboratoire Paul Painlevé
Université de Lille
Cité Scientifique, Bâtiment M2
59650 Villeneuve-d'Ascq, France.
email: an.iadarola@gmail.com

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 4, *Number* 1, *March* 2019, *pages* 49-59

Elisa Lorenzo García

Primes of bad reduction of CM curves of genus 3

Written by Guido Maria Lido

1 Introduction

The aim of this talk is to present some recent results bounding the primes of bad reduction for a CM curve of genus 3. Before looking at this problem we will look at the analogue for curves of genus 1 and curves of genus 2 in order to give motivation in a more familiar context.

2 Hilbert class polynomial and good reduction of CM elliptic curves

If we fix an algebraically closed field k, all elliptic curves over k up to isomorphism can be parametrized with a single invariant called j-invariant. For example if the characteristic of k is different from 2 or 3 every elliptic curve E over k has a Weierstrass model

$$y^2 = x^3 + Ax + B$$

for certain $A, B \in k$ such that $4A^3 + 27B^3 \neq 0$ and we can write the j-invariant of E as

$$j(E) = -1728\frac{(4A)^3}{\Delta(E)} = -1728\frac{(4A)^3}{16(4A^3 + 27B^2)}.$$

If we consider the endomorphism ring of an elliptic curve E we know that there are three kinds of possibilities:

1. $\mathrm{End}(E) \cong \mathbb{Z}$, if the only endomorphisms are of the form $[n] : P \to P + \cdots + P$;

2. End(E) is isomorphic to an order $\mathcal{O}$ in an quadratic imaginary number field; every such order $\mathcal{O}$ is of the form $\mathbb{Z}[\frac{\sqrt{D}+D}{2}]$ for some negative integer D not congruent to 3 (mod 4);

3. $\mathrm{End}(E)$ is an order inside a quaternion algebra $\mathcal{B}$; this can only happen in positive characteristic and if $p = char(k)$ then $\mathcal{B}$ is the only quaternion algebra over $\mathbb{Q}$ such that $\mathcal{B} \otimes \mathbb{Q}_v$ is isomorphic to $\mathrm{Mat}_{2\times 2}(\mathbb{Q}_v)$ for all rational places in v except from ∞ and p; We will denote it as $\mathcal{B}_{p,\infty}$.

In characteristic zero there are two kinds of elliptic curves: ordinary elliptic curves (case 1) and elliptic curves with *complex multiplication* (case 2). Let us now recall some "classical" facts about complex multiplication whose proof can be found in the second chapter of [10]. Since any elliptic curve with CM defined over a field k of characteristic zero is isomorphic to an elliptic curve defined over the algebraic numbers, we only need to look at curves defined over $\overline{\mathbb{Q}}$.

Proposition 1 *Let $\mathcal{O}$ be an order in a quadratic imaginary field. Then:*

1. *there exists an elliptic curve E over $\overline{\mathbb{Q}}$ such that* $\mathrm{End}(E) = \mathcal{O}$*;*

2. *if E over $\overline{\mathbb{Q}}$ is any elliptic curve such that* $\mathrm{End}(E) = \mathcal{O}$*, then the set*

$$\left\{(E)^\sigma : \ \sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})\right\}$$

is equal to the set of all elliptic curves E' over $\overline{\mathbb{Q}}$ such that $\mathrm{End}(E') = \mathcal{O}$*, up to isomorphism.*

3. *if E is an elliptic curve with complex multiplication defined over a number field L, then E has potential good reduction over any prime $\mathcal{P} \subset \mathcal{O}_L$; in particular $j(E)$ is an algebraic integer.*

The second point of proposition 1 implies that up to isomorphism there are only finitely many elliptic curves over $\overline{\mathbb{Q}}$ with ring of endomorphism a fixed order $\mathcal{O}$, thus we can give the following definition.

Definition 1 *Given an order $\mathcal{O}$ inside a quadratic imaginary field we define the* modular polynomial relative to $\mathcal{O}$ *to be*

$$H_{\mathcal{O}}(X) = \prod_{E:\ \mathrm{End}(E)=\mathcal{O}} \Big(X - j(E)\Big)$$

where the product is taken over the set of elliptic curves E such that $\mathrm{End}(E) = \mathcal{O}$*, up to isomorphism.*

A motivation for studying and computing modular polynomials is given by cryptography, since they can be used to construct elliptic curves over finite fields with a given number of rational points. Proposition 1 implies that $H_{\mathcal{O}}(X)$ is an irreducible polynomial with coefficients in $\mathbb{Z}$. Let us see how to exploit this, together with some tools from complex analysis, to compute modular polynomials.

Every elliptic curve E over $\mathbb{C}$ is isomorphic as a complex manifold to a complex torus of the form $\mathbb{C}/\langle 1, \tau\rangle$ for some τ in

$$\mathcal{H} = \{\tau \in \mathbb{C} :\ \ \mathrm{Im}(\tau) > 0\}.$$

Moreover we can write the j-invariant of E as the value in τ of an analytic function $J : \mathcal{H} \to \mathbb{C}$ (not depending on τ), i.e.

$$j(E) = J(\tau) = e^{-2\pi i\tau} + 744 + 196884e^{2\pi i\tau} + 21493760e^{4\pi i\tau} + \dots$$

Since the function J is effectively computable, in order to compute the modular polynomial relative to an order $\mathcal{O}$ we can do the following

1. Compute $\tau_1, \ldots, \tau_n \in \mathcal{H}$ with the following property: every elliptic curve E over $\mathbb{C}$ such that $\mathrm{End}(E) = \mathcal{O}$ is analytically isomorphic to $\mathbb{C}/\langle 1, \tau_i \rangle$ for a unique $i \in \{1, \ldots n\}$;

2. Compute an approximation $\tilde{j}_i$ of $J(\tau_i)$ up to sufficiently good precision (it is enough $2^{-n-1} \max_i\{|j(\tau_i)|\} \leq 2^{-n-1}$);

3. Compute the polynomial

$$\tilde{H}(X) = \prod_{i=1}^{n}(X - \tilde{j}_i)$$

and approximate it with the polynomial $H \in \mathbb{Z}[X]$ whose coefficients are as close as possible to the polynomial $\tilde{H}$.

The polynomial H computed in the third step is equal to the modular polynomial $H_{\mathcal{O}}$. Indeed if we call $\tilde{c}_k$'s and c_k's the coefficients respectively of $\tilde{H}(X)$ and $H_{\mathcal{O}}(X)$, then $|c_k - \tilde{c}_k| < \frac{1}{2}$ and since the c_k's are integral, we conclude that

$$H = H_{\mathcal{O}}$$

.

3 Igusa class polynomial and bad reduction of genus 2 CM curves

Let us now consider algebraic curves of genus 2 over a field k of characteristic different from 2 or 3. Any such curve C has an affine model of the form $y^2 = f(x)$ where $f \in k[x]$ is a separable polynomial of degree 6.

For any polynomial $f \in k[x]$ of degree 6 we denote $\alpha_1, \ldots, \alpha_6 \in \overline{k}$ the roots of f and we define the following quantities:

$$\Delta = \prod_{1 \leq i < j \leq 6} (\alpha_i - \alpha_j)^2$$

$$I_1 = \sum_{sym} (\alpha_1 - \alpha_2)^2(\alpha_3 - \alpha_4)^2(\alpha_5 - \alpha_6)^2$$

$$I_2 = \sum_{sym} (\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2(\alpha_4 - \alpha_5)^2(\alpha_4 - \alpha_6)^2(\alpha_5 - \alpha_6)^2$$

$$I_3 = \sum_{sym} \frac{\Delta}{(\alpha_1 - \alpha_5)^2(\alpha_1 - \alpha_6)^2(\alpha_2 - \alpha_4)^2(\alpha_2 - \alpha_6)^2(\alpha_3 - \alpha_4)^2(\alpha_3 - \alpha_5)^2}$$

$$I_3' = 5I_1I_2 - 2^5 3^3 I_3$$

where "$\sum_{sym}$" means that we sum over all the permutations of $\alpha_1, \ldots, \alpha_6$. Given a curve $C : y^2 = f(x)$ the Igusa invariants of C are defined in [4] as

$$j_1 = \frac{I_2 I_3'}{2^{10} \cdot 3^5 \cdot 5 \cdot \Delta}, \quad j_2 = \frac{I_1 I_2^2}{2^8 \cdot 3^5 \cdot \Delta} \quad j_3 = \frac{I_2^5}{2^{15} \cdot 3^{10} \cdot \Delta^2}.$$

Analogously to what happens for elliptic curves and the j-invariant, two genus 2 curves $C_1 : y^2 = f_1(x)$ and $C_2 : y^2 = f_2(x)$ are isomorphic over $\overline{k}$ if and only if they have the same Igusa invariants. Moreover if k happens to be a number field and $\mathfrak{p}$ is a prime of k, then a curve C has potential good reduction modulo $\mathfrak{p}$ if and only if all Igusa invariants of C are $\mathfrak{p}$-integral.

Another analogy with the j-invariant of elliptic curves is that we can compute the Igusa invariants of a genus 2 curves in terms of a holomorphic function on a complex moduli space. Indeed if we define

$$\mathcal{H}_2 = \left\{ \tau \in M^{2\times 2}(\mathbb{C}) : \quad \tau = \tau^t, \ \ \mathrm{Im}(\tau) \text{ is positive definite} \right\}$$

then for each genus 2 curve C over the complex numbers, there is a $\tau = \left(\tau_1 | \tau_2\right) \in \mathcal{H}_2$ such that $\mathrm{Jac}(C) \cong \mathbb{C}^2 / \langle e_1, e_2, \tau_1, \tau_2 \rangle$ as principally polarized Abelian variety. Moreover there are holomorphic functions $J_1, J_2, J_3 : \mathcal{H}_2 \to \mathbb{C}$ such that $j_i(C) = J_i(\tau)$.

As in the case of elliptic curves we can define a class polynomial for genus 2 curves. Let us give some preliminary definition.

Definition 2 *A number field K is a* CM-field *if it is a totally imaginary quadratic extension of a totally real field K^+*

Definition 3 *A curve C of genus g defined over $\overline{\mathbb{Q}}$ is a* CM curve *if there exists a CM-field K of degree $2g$ and an order $\mathcal{O} \subset K$ such that*

$$\mathcal{O} \subset \mathrm{End}\Big(\mathrm{Jac}(C)\Big).$$

In this case we say that C has complex multiplication by $\mathcal{O}$.

Given a fixed order $\mathcal{O}$ inside a quartic CM-field K there are only finitely many curves of genus 2 over $\overline{\mathbb{Q}}$ having complex multiplication by $\mathcal{O}$ up to isomorphism. We can then define three *Class polynomials* $H^1_{\mathcal{O}}, H^2_{\mathcal{O}}, H^3_{\mathcal{O}}$ with the following formulas

$$H^i_{\mathcal{O}}(X) = \prod_{\substack{\mathrm{End}\left(\mathrm{Jac}(C)\right) \cong \mathcal{O} \\ g(C)=2}} \Big(X - j_i(C)\Big).$$

It is easy to show that Class polynomials $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-invariant, i.e. that they have coefficients in $\mathbb{Q}$: indeed if C is a genus 2 curve with CM by $\mathcal{O}$, then for any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ the curve C^σ is also a genus 2 curve with CM by $\mathcal{O}$; thus if j_i is a root of $H^i_{\mathcal{O}}$ then each Galois-conjugate of j_i is also a root of $H^i_{\mathcal{O}}$.

Unfortunately it is not true that a CM curve C has potential good reduction everywhere, i.e. that the invariants $j_i(C)$ are algebraic integers. Indeed the Class polynomials $H^i_{\mathcal{O}}$ may have non-integral coefficient. Anyway if we had a bound B for the denominators of the coefficients of $H^i_{\mathcal{O}}$ we could compute $H^i_{\mathcal{O}}$ with an algorithm similar to the one for elliptic curves, since all the other ingredients are still available. Such bounds have been given by Goren, Lauter and Viray, by bounding the denominators of the Igusa invariants of the curves involved. Indeed in [2] it is proved the following

Theorem 1 *Let C be a genus 2 curve with complex multiplication by an order $\mathcal{O}$ inside a a quartic CM-field K not containing any quadratic imaginary subfield. Then we can write*

$$K = \mathbb{Q}(\sqrt{d})(\sqrt{r})$$

for some $d \in \mathbb{Z}$ and some $r \in \mathbb{Q}(\sqrt{d}) \cap \mathcal{O}$ both totally real. If C has geometrical bad reduction for a prime lying over p, then

$$p < 16d^2(\mathrm{Tr}(r))^2.$$

To finish the work one also needs to bound the valuation of the Igusa invariants in the primes of bad reduction. This has been done for example in [3] achieving the following bounds for the denominators of the Class polynomials relative to some maximal orders $\mathcal{O}_K$.

Theorem 2 *Let K be a quartic CM-field not containing any quadratic imaginary subfield and let p ne any prime. In particular we can write*

$$K = \mathbb{Q}(\sqrt{d})(\sqrt{r})$$

for some $d \in \mathbb{Z}$ and some $r \in \mathbb{Q}(\sqrt{d}) \cap \mathcal{O}$ both totally real. Then the valuations at p of the coefficients of $H^1_{\mathcal{O}_K}, H^2_{\mathcal{O}_K}, H_{\mathcal{O}_K}$ are at least

$$-16 \deg H^1_{\mathcal{O}_K} \left(4 \log_p \left(\frac{d\,\mathrm{Tr}(r)^2}{2}\right) + 1\right)$$

Instead of explaining the strategy used to prove the last two theorems we will now look at analogous results for genus 3 curves and at the ideas used to prove those.

4 Bad reduction of genus 3 CM curves and the embedding problem

The definition of CM curves in genus 3 is just a particular case of definition 3, but there are some substantial differences with the case of

genus 2 curves, indicating that finding such bounds is a necessary but not sufficient step, if we want to compute class polynomials in genus 3. One of the missing ingredients is the analogue of Igusa invariants, since we do not know good coordinates for the moduli space of curves of genus 3. Indeed we can distinguish between two kinds of genus 3 curves, each one with its own invariants:

- hyperelliptic genus 3 curves: in characteristic different from 2 they all have a model $y^2 = f(x)$ for a separable polynomial f of degree 8; Shioda defined invariants in [9] for this kind of curves.
- non-hyperelliptic genus 3 curves: they are all isomorphic to a smooth projective plane quartic; invariants for this family of curves where defined by Dixmier and Ohno in [1] and [8].

Another difference is that in general integrality of the invariants of a genus 3 curve is not equivalent to potential good reduction of the curve. This is true for hyperelliptic curves, but not in general for smooth plane quartics. For example it may happen that C is a CM non-hyperelliptic curve of genus 3 that has potential good reduction of C modulo some prime $\mathfrak{p}$ but that the reduction of the curve is hyperelliptic; in this case one of the invariants is not $\mathfrak{p}$-integral.

In the rest of this section we will see some partial results that give bounds on the bad reduction of CM curves of genus 3. To state precisely our results we need to define a notion of "primitivity".

Definition 4 *Let ρ be usual conjugation on $\mathbb{C}$. A* CM-type *is a pair (K, ϕ) such that K is a CM-field and ϕ is a set of embeddings $K \hookrightarrow \mathbb{C}$ such that*

$$\mathrm{Hom}(K, \mathbb{C}) = \phi \cup \rho\phi, \quad \textit{and} \quad \phi \cap \rho\phi = \emptyset$$

Definition 5 *A CM-type (K, ϕ) is* primitive *if there is no proper subfield $E \subset K$ such that $(E, \phi|_E)$ is a CM-type.*

In [7] it is explained how one can define the CM-type associated to a CM Abelian variety $A/\mathbb{C}$. We say that a CM curve has primitive

CM-type if the CM-type associated to its Jacobian is primitive.

Let us now return to our main problem. Let C be a semistable CM curve of genus 3 with Jacobian J and let p be a prime of bad reduction for p. One of the ideas in [2] was to look at the reduction of J modulo p: by a theorem of Serre and Tate it is still an Abelian variety and the hypothesis on p implies that it is isogenous to the third power of a supersingular elliptic curve. If we reduce the endomorphisms of J modulo p, we step into the following, purely algebraic problem.

Problem 1 (Embedding problem for $\mathcal{O}$ and p) *Given an order $\mathcal{O}$ inside a CM sextic field and a prime p does there exist an embedding*

$$\iota : \mathcal{O} \hookrightarrow \mathrm{Mat}_{3\times 3}(\mathcal{B}_{p,\infty}) \qquad ?$$

The precise relation between the embedding problem and our original problem is in the following proposition proved in [5].

Proposition 2 *Let C be a curve a genus 3 with CM by an order $\mathcal{O}$ and primitive CM type. Suppose that C has geometric bad reduction over a prime lying over p. Then we can find $\alpha, \gamma \in \mathbb{Z}$, $\beta \in \mathcal{B}_{p,\infty}$ and an embedding $\iota : \mathcal{O} \hookrightarrow \mathrm{Mat}_{3\times 3}(\mathcal{B}_{p,\infty})$ such that*

$$\alpha\gamma \neq \beta\beta^{\vee} \quad \text{and}$$

$$\iota(\overline{\eta}) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \alpha & \beta \\ 0 & \beta^{\vee} & \gamma \end{pmatrix}^{-1} \cdot \left(\iota(\eta)^{\vee}\right)^{t} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & \alpha & \beta \\ 0 & \beta^{\vee} & \gamma \end{pmatrix}$$

where $^{\vee} : \mathcal{B}_{p,\infty} \to \mathcal{B}_{p,\infty}$ is the canonical involution.

In [5] it is proven that the (complicated version of the) embedding problem has no solution for large p, implying the following

Theorem 3 *with CM by an order $\mathcal{O}$ and primitive CM type. Suppose that C has bas reduction over a prime lying over p. Then for every $\mu \in \mathcal{O}$ with μ^2 totally real and $K = Q(\mu)$, we have*

$$p < \frac{1}{2^{13}}\left(\mathrm{Tr}_{K/\mathbb{Q}}(\mu)\right)^{10}.$$

Let us now turn to the problem of bounding from below the valuation $v_{\mathfrak{p}}(j)$ when j is the invariant of a curve having CM by a particular order $\mathcal{O}$ and $\mathfrak{p}$ is a prime. For curves of genus 2 this was obtained in [6] by relating this valuation to the number of solutions of the embedding problem. At the moment there are no similar formulas for genus 3 curves, while bounding the number of possible embeddings is the aim of an ongoing project by Garcia, Ionica, Kiliçer, Lauter, Massierer, Mânzăţenau and Vincent. One of the results of this work is a bound on the number of the embeddings and an algorithm that computes all of them. This has been achieved in a very explicit way: if we fix $\mu \in \mathcal{O}$ that generates the sextic CM field and that satisfies a relation $\mu^6 + A\mu^4 + B\mu^2 + C = 0$ over the integers, then finding all the embeddings is equivalent to solving the following system of equations in $\alpha, \beta, \gamma, d, x \in \mathcal{B}_{p,\infty}$ and $n \in \mathbb{Z}_{>0}$:

$$
\begin{aligned}
A =& \operatorname{N}(x) + \operatorname{Tr}(\alpha) + \operatorname{Tr}(\gamma)/\alpha + \operatorname{Tr}(\beta d)/(\alpha n) + \operatorname{N}(d/n),\\
B =& \alpha^2 + 2n/\alpha + 2n\operatorname{N}(x)/\alpha^2 + 2\alpha\operatorname{N}(d/n) + 2\operatorname{N}(b)/\alpha + \operatorname{Tr}(x\beta) +\\
& 2\operatorname{Tr}(d\beta/n) + n\operatorname{Tr}(d\beta/n)/\alpha^3 + N(x)N(d/n) + N(x)\operatorname{Tr}(d\beta/n)/\alpha +\\
& \big(\operatorname{N}(d/n) + 2\operatorname{N}(x)\big)N(\beta)/\alpha^2 + N(\beta)\operatorname{Tr}(d\beta/n)/\alpha^3 + \operatorname{N}(\gamma)/\alpha^2,\\
C =& \operatorname{N}\Big(- x\gamma/\alpha - x\beta d/(\alpha n) - \alpha d/n + \beta\Big).
\end{aligned}
$$

For example if $K = \mathbb{Q}[t]/(t^6 + 13t^4 + 50t^2 + 49)$ then there is only one curve of genus 3 and CM by $\mathcal{O}_K$ (indeed K has class number 1), i.e.

$$C: \quad y^2 = x^7 + 1786x^5 + 44441x^3 + 278179x$$

with $\Delta = 2^{18} \cdot 7^{24} \cdot 11^{12} \cdot 19^7$. Actually only 7 and 11 are primes of geometric bad reduction: for $p = 7$ there are two solutions to the embedding problem, for $p = 11$ there is only one.

References

[1] J. Dixmier, *On the projective invariants of quartic plane curves*. Adv. in Math., 64(3):279-304, 1987.

[2] E. Goren, K. Lauter, *Class invariants for quartic CM fields*. Ann. Inst. Fourier, 57(2):457-480, (2007).

[3] E. Z. Goren and K. E. Lauter., *Genus 2 curves with complex multiplication*. Inter. Math. Research Notices 5:1068-1142, 2012.

[4] J. I. Igusa., *Arithmetic variety of moduli for genus two*. Annals of Math., 72(3):612-649, 1960.

[5] P. Kiliçer, K. Lauter, E. Lorenzo García, R. Newton, E. Ozman, M. Streng, *A bound on the primes of bad reduction for CM curves of genus 3*. Preprint arXiv:1609.05826, (2018)

[6] K. Lauter, B. Viray, *An arithmetic intersection formula for denominators of Igusa class polynomials*. American Journal of Math., 137(2):497-533, 2015.

[7] J. S. Milne, *Complex multiplication*. Lectures Notes available on line: http://www.jmilne.org/math/CourseNotes/cm.html, 2006.

[8] T. Ohno, *Invariant subring of ternary quartics I generators and relations*. Preprint, https://www.win.tue.nl/ aeb/math/ohno-preprint.2007.05.15.pdf, 2007.

[9] T. Shioda., *On the graded ring of invariants of binary octavics*. American Journal of Math., 89:1022-1046, 1967.

[10] J. H. Silvermann, *Advanced topics in the arithmetic of elliptic curves*. Graduate texts in math, 151, 1994.

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 4, *Number* 1, *March* 2019, *pages* 61-65

René Schoof

Heights and principal ideals of certain cyclotomic fields

Written by Peter Lombaers

Let G be a finite group and suppose we want to find a field extension which has G as its Galois group. One approach would be to embed G into the symmetric S_n for some some natural number n. Let the group S_n act on the field $\mathbb{Q}(X_1, \ldots, X_n)$ by permuting the indeterminates X_i. Then the field extension $\mathbb{Q}(X_1, \ldots, X_n)/\mathbb{Q}(X_1, \ldots, X_n)^G$ has Galois group G.

However, we would like to find an extension of $\mathbb{Q}$ with Galois group G. If $\mathbb{Q}(X_1, \ldots, X_n)^G$ is purely transcedental over $\mathbb{Q}$, then we can use Hilbert's irreducibility theorem to find extensions of $\mathbb{Q}$ with Galois group G. In the case where G is the symmetric group S_n or the alternating group A_n, this approach indeed works.

This leads to *Noether's problem for G over* $\mathbb{Q}$: for which finite groups G is $\mathbb{Q}(X_1, \ldots, X_n)^G/\mathbb{Q}$ purely transcedental? A natural place to start is by looking at the cylic group C_n. Let P be the set of all primes p such that $\mathbb{Q}(X_1, \ldots, X_n)^G/\mathbb{Q}$ purely transcedental for $G = C_p$. The first few small primes are all in P, but in 1969 Richard Swan showed that 47 is not. In fact, in 1974, Hendrik Lenstra showed that the density of P in the set of all primes is equal to 0 [3]. He also showed that p is in P if and only if the field $\mathbb{Q}(\zeta_{p-1})$ contains an element with

norm p. Here ζ_n is a primitive n'th root of unity. The prime p splits completely in the extension $\mathbb{Q}(\zeta_{p-1})/\mathbb{Q}$, i.e. $p\mathbb{Z}[\zeta_{p-1}] = \mathfrak{p}_1 \dots \mathfrak{p}_r$, where $r = [\mathbb{Q}(\zeta_{p-1} : \mathbb{Q}] = \phi(p-1)$. Hence the question becomes: For which p are these ideals $\mathfrak{p}$ principal?

Example 1 *If $p = 5$, then $\mathbb{Q}(\zeta_{p-1}) = \mathbb{Q}(i)$ and $5 = (2+i)(2-i)$, so 5 splits into principal ideals. If $p = 47$, then $\mathbb{Q}(\zeta_{p-1}) = \mathbb{Q}(\zeta_{23})$, which contains $\mathbb{Q}(\sqrt{-23})$ as a subfield. We can use binary quadratic forms to show that the ideals of $\mathbb{Q}(\sqrt{-23})$ above 47 are not principal. Note that $2x^2 + xy + 3y^2$ is not a principal binary quadratic form, but by taking $(x, y) = (4, -3)$ we see that it represents 47. So the ideals above 47 are not principal in $\mathbb{Q}(\sqrt{-23})$ and therefore also not in $\mathbb{Q}(\zeta_{23})$.*

The complete answer to the question was recently given by Bernat Plans [4].

Theorem 1 (Plans) *An ideal $\mathfrak{p}$ of $\mathbb{Q}(\zeta_{p-1})$ above p is principal if and only if $\mathbb{Q}(\zeta_{p-1})$ has class number one, so if and only if*

$$p \in \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 61, 67, 71\}.$$

In the rest of this text we shall have a look at the proof of this theorem. Of course if $\mathbb{Q}(\zeta_{p-1})$ has class number one, then all ideals are principal, so in particular $\mathfrak{p}$. For the other direction we need to introduce heights.

Let K be a number field and let $\alpha \in K^*$. We normalize the valuations of K as follows. If v is a finite prime corresponding then $|\alpha|_v = q^{-v(\alpha)}$ where q is the number of elements in the residue field. If v corresponds to a real embedding $i : K \to \mathbb{R}$ then $|\alpha|_v = |i(\alpha)|_{\mathbb{R}}$. If v corresponds to a complex embedding $i : K \to \mathbb{C}$ then $|\alpha|_v = |i(\alpha)|^2_{\mathbb{C}}$. In this way the product formula $\prod_v |\alpha|_v = 1$ holds.

Define the height $h(\alpha)$ of α as

$$h(\alpha) := \log \prod_v \max(1, |\alpha|_v).$$

Here the product is over all valuations of K. For example in $\mathbb{Q}$ we see $h(\frac{a}{b}) = \log(\max(|a|, |b|))$ if a and b are relatively prime. If L/K is finite field extension then $h_L(\alpha) = [L : K]h_K(\alpha)$. Hence $h(\alpha)$ depends on the field K, but the absolute height $h(\alpha)/[K : \mathbb{Q}]$ only depends on α.

Some basic properties of h are that we always have $h(\alpha) \geq 0$ and we have $h(\alpha) = 0$ if and only if α is a root of unity. Lehmer's conjecture says that there is a positive constant which bounds the absolute height from below. In general this is a conjecture, but for cyclotomic fields we have the following result [1]:

Theorem 2 (Amoroso-Dvornicich) *For $\alpha \in \mathbb{Q}(\zeta_n)$ not a root of unity and for all primes q we have*

$$\frac{h(\alpha)}{\phi(n)} > \frac{\log(q/2)}{2q}.$$

If $q \nmid n$ then

$$\frac{h(\alpha)}{\phi(n)} > \frac{\log(q/2)}{q+1}.$$

We obtain the best lower bound using $q = 5$, which gives $\frac{h(\alpha)}{\phi(n)} > 0.09$. We will now show how Theorem 1 follows from the result of Amoroso and Dvornicich.

*(Sketch of proof of Theorem 1).*Suppose that p splits into principal ideals in $\mathbb{Q}(\zeta_{p-1})$, so $p\mathbb{Z}[\zeta_{p-1}] = (\pi_1) \dots (\pi_{\phi(p-1)})$. Let $\pi = \pi_1$ and consider the element $\frac{\pi}{\overline{\pi}}$. Here $\overline{\pi}$ is the complex conjugate of π. Since $|\frac{\pi}{\overline{\pi}}|_v = 1$ for the archimedean valuations, we find that $h(\frac{\pi}{\overline{\pi}}) = \log p$.

Because p splits completely, (π) and $(\overline{\pi})$ must be different ideals and thus $\frac{\pi}{\overline{\pi}}$ is not a unit. In particular it is not a root of unity, so by Amoroso-Dvornicich we see

$$\frac{\log p}{\phi(p-1)} > 0.09$$

Since $\phi(n)$ grows faster than $\log n$, this leaves us with a finite list of possible primes. For these primes we can use the second bound of Theorem 2, after which we are left with the primes $47, 53, 73$ and 79. In the original, Plans got rid of the exceptions by using computer calculations done by Hoshi [2]. Alternatively these cases can be done by hand. In the example above we used binary quadratic forms to show 47 does not split into principal ideals in $\mathbb{Q}(\sqrt{-23})$. The case $p = 53$ can be done in similar fashion. The final two cases can be done by considering suitable subfields of $\mathbb{Q}(\zeta_{72})$ and $\mathbb{Q}(\zeta_{39})$ and using class field theory.

□

Finally we will give an idea of how the prove the theorem by Amoroso and Dvornicich. We need the following lemma, which basically follows from the product formula.

Lemma 1 *Let F be a number field, $x, y \in F^*$ with $x \neq y$ and let q be a prime integer. If for any valuation $v|q$ we have*

$$|x - y|_v \leq |q|_v \max(1, |x|_v) \max(1, |y|_v)$$

then

$$\frac{h(x) + h(y)}{[F : \mathbb{Q}]} \geq \log(\frac{q}{2}).$$

In the case where $q \nmid n$, we apply this lemma to $x = \alpha^q$ and $y = \sigma(\alpha)$ where σ is the Frobenius automorphism corresponding to q. Since $h(\alpha^q) = qh(\alpha)$ and $h(\sigma(\alpha)) = h(\alpha)$, the theorem follows immediately after we show that α^q and $\sigma(\alpha)$ satisfy the conditions of the lemma.

Let $v|q$ be a valuation. By the strong approximation theorem we can find an algebraic integer β such that $\alpha\beta$ is an algebraic integer and $|\beta|_v = \max(1, |\alpha|_v)^{-1}$. Then $|\sigma(\beta) - \beta^q|_v \leq |q|_v$ and $|\sigma(\alpha\beta) - (\alpha\beta)^q|_v \leq |q|_v$ because σ is the Frobenius automorphism. This leads to the desired inequality:

$$\begin{aligned} |\alpha^q - \sigma(\alpha)|_v &= |\beta|_v^{-q} |(\alpha\beta)^q - \sigma(\alpha\beta) + (\sigma\beta - \beta^q)\sigma(\alpha)|_v \\ &\leq |\beta|_v^{-q} \max(|(\alpha\beta)^q - \sigma(\alpha\beta)|_v, |\sigma(\beta) - \beta^q|_v |\sigma(\alpha)|_v) \\ &\leq |q|_v \max(1, |\alpha^q|_v) \max(1, |\sigma(\alpha)|_v) \end{aligned}$$

In the case where q divides n, there no longer exists a Frobenius automorphism corresponding to q, so we need to pick different x and y. Let σ be a generator of the cyclic group $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_{\frac{n}{q}}))$. Then σ fixes ζ_n^q and thus $\sigma(\alpha)^q \equiv \alpha^q \mod q$. Hence we choose $x = \alpha^q$ and $y = \sigma(\alpha)^q$. A similar argument as before shows that the conditions of the lemma are satisfied and the theorem follows immediately.

References

[1] F. Amoroso and R. Dvornicich, *A lower bound for the height in abelian extensions*, *J. Number theory.* 80(2):260–272, 2000.

[2] A. Hoshi, *On Noether's problem for cyclic groups of prime order*, *Proc. Japan Acad. Ser. A.* 91:39–44, 2015.

[3] H. W. Lenstra Jr., *Rational functions invariant under a finite abelian group*, *Invent. Math.* 25:299–325, 1974.

[4] B. Plans, *On Noether's rationality problem for cyclic groups over* $\mathbb{Q}$, *Proc. Amer. Math. Soc.* 145(6):2407–2409, 2017.

Peter Lombaers
Departamento de Matemática da FCUP
Universidade do Porto
Rua do Campo Alegre 687
4169-007, Porto, Portugal.
email: p.lombaers@gmail.com

IT36Z0760103200000027923010

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 4, *Number* 1, *March* 2019, *pages* 67-72

Amir Akbary

Value-distribution of cubic L-functions

Written by Andam Mustafa

This is a report of the results obtained in a joint work by Amir Akbary and Alia Hamieh. The study on the distribution of values of L-functions associated with quadratic Dirichlet characters in the half plane $\Re(s) > \frac{1}{2}$ has been investigated by several authors. One of the early results is obtained by Chowla and Erdős in 1953. Let d be an integer such that d is not a perfect square and $d \equiv 0, 1 \pmod 4$. Suppose that, for $\Re(s) > 0$, we have

$$L_d(s) = \sum_{n=1}^{\infty} \frac{\left(\frac{d}{n}\right)}{n^s}.$$

Here the quadratic Dirichlet character of the function $L_d(s)$ is determined by the Kronecker symbol $\left(\frac{d}{\cdot}\right)$. The distribution of values of $L_d(s)$ in the half-line $\sigma > \frac{3}{4}$ for varying d has been described by the authors in [1] as the following theorem.

Theorem 1 (Chowla-Erdős) *If $\sigma > 3/4$, we have*

$$\lim_{x\to\infty} \frac{\#\{0 < d \le x; d \equiv 0, 1 \pmod 4 \text{ and } L_d(\sigma)\} \le z\}}{x/2} = G(z),$$

where $G(0) = 0, G(\infty) = 1$ and $G(z)$ is the distribution function, which is a continuous and strictly increasing function of z.

In 1970 Elliott reconsidered this problem for $\sigma = 1$ and extended Chowla-Erdős theorem. The following is proved in [2].

Theorem 2 (Elliott) *There is a distribution function $F(z)$ such that*

$$\frac{\#\{0 < -d \le x; d \equiv 0, 1 \pmod 4 \text{ and } L_d(1) \le z\}}{x/2} = F(z) + O\left(\sqrt{\frac{\log\log x}{\log x}}\right)$$

holds uniformly for all real z, and real $x \ge 9$. $F(z)$ has a probability density, may be differentiated any number of times, and has the characteristic function

$$\varphi_F(y) = \prod_p \left(\frac{1}{p} + \frac{1}{2}\left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{p}\right)^{-iy} + \frac{1}{2}\left(1 - \frac{1}{p}\right)\left(1 + \frac{1}{p}\right)^{-iy}\right)$$

which belongs to the Lebesgue class $L^1(-\infty, \infty)$.

This theorem provides detailed information on the distribution function in Chowla-Erdős theorem for $\sigma = 1$ with an explicit error term. In 1970 Elliott explored similar expressions for several other functions (see [3, 4, 5]).

In 2015, Mourtada and Murty [6] described the density function M_σ for the values of the logarithmic derivative of $L_d(s)$ for $\sigma > \frac{1}{2}$ in the following theorem.

Theorem 3 (Mourtada-Murty) *Let $\sigma > \frac{1}{2}$ and assume the GRH (the Generalized Riemann Hypothesis for $L_d(s)$). Let $\mathcal{F}(Y)$ denote the set of the fundamental discriminants in the interval $[-Y, Y]$ and let $N(Y) = \#\mathcal{F}(Y)$. Then, there exists a probability density function M_σ, such that*

$$\lim_{Y\to\infty} \frac{1}{N(Y)} \#\{d \in \mathcal{F}(Y); (L_d'/L_d)(\sigma) \le z\} = \int_{-\infty}^{z} M_\sigma(t)dt.$$

Moreover, the characteristic function $\varphi_{F_\sigma}(y)$ of the asymptotic distribution function $F_\sigma(z) = \int_{-\infty}^{z} M_\sigma(t)dt$ is given by

$$\varphi_{F_\sigma}(y) = \prod_p \left(\frac{1}{p+1} + \frac{p}{2(p+1)} \exp\left(-\frac{iy \log p}{p^\sigma - 1} \right) + \frac{p}{2(p+1)} \exp\left(\frac{iy \log p}{p^\sigma + 1} \right) \right).$$

Here Amir Akbary and Alia Hamieh note that it is possible to remove the GRH assumption in Theorem 3 by applying an appropriate zero density theorem for L-functions of quadratic Dirichlet characters. They describe their approach for certain cubic L-functions.

Notice that if d is a fundamental discriminant then

$$L_d(s) = \frac{\zeta_{\mathbb{Q}(\sqrt{d})}(s)}{\zeta(s)}, \tag{1}$$

where $\zeta_{\mathbb{Q}(\sqrt{d})}(s)$ is the Dedekind zeta function of $\mathbb{Q}(\sqrt{d})$ and $\zeta(s)$ is the Riemann zeta function. For $k = \mathbb{Q}(\sqrt{-3})$, let $\mathfrak{O}_k = \mathbb{Z}[\zeta_3]$ be the ring of integers of k, where $\zeta_3 = e^{\frac{2\pi i}{3}}$. Let

$$C := \{c \in \mathfrak{O}_k; c \neq 1 \text{is square free and } c \equiv 1 \pmod{\langle 9 \rangle}\}.$$

Similar to (1), we can define

$$L_c(s) = \frac{\zeta_{k(c^{1/3})}(s)}{\zeta_k(s)}, \tag{2}$$

where $\zeta_{k(c^{1/3})}(s)$ is the Dedekind zeta function of the cubic field $k(c^{1/3})$ for $c \in C$.

We set

$$\mathcal{L}_c(s) = \begin{cases} \log L_c(s) & \text{(Case 1)}, \\ (L_c'/L_c)(s) & \text{(Case 2)}. \end{cases}$$

The following was the main result of this talk.

Theorem 4 (Akbary-Hamieh) *Let $\sigma > \frac{1}{2}$. Let $\mathcal{N}(Y)$ be the the number of elements $c \in C$ with norm not exceeding Y. There exists a smooth density function M_σ such that*

$$\lim_{Y\to\infty} \frac{1}{\mathcal{N}(Y)} \#\{c \in C : N(c) \le Y \text{and } \mathcal{L}_c(\sigma) \le z\} = \int_{-\infty}^{z} M_\sigma(t)dt.$$

The asymptotic distribution function $F_\sigma(z) = \int_{-\infty}^{z} M_\sigma(t)dt$ can be constructed as an infinite convolution over prime ideals $\mathfrak{p}$ of k,

$$F_\sigma(z) = *_{\mathfrak{p}} F_{\sigma,\mathfrak{p}}(z),$$

where

$$F_{\sigma,\mathfrak{p}}(z) = \begin{cases} \dfrac{1}{N(\mathfrak{p})+1}\delta + \frac{1}{3}\left(\dfrac{N(\mathfrak{p})}{N(\mathfrak{p})+1}\right)\sum_{j=0}^{2}\delta_{-a_{\mathfrak{p},j}}(z) & \text{if } \mathfrak{p} \nmid \langle 3\rangle, \\ \delta_{a_{\mathfrak{p},0}}(z) & \text{if } \mathfrak{p} \nmid \langle 1-\zeta_3\rangle. \end{cases}$$

Here $\delta_a := \delta(z-a)$, δ is the Dirac distribution, and

$$a_{\mathfrak{p},j} := a_{\mathfrak{p},j}(\sigma) = \begin{cases} 2\Re\left(\log(1-\zeta_3^j N(\mathfrak{p})^{-\sigma}\right) & \text{in (Case 1)}, \\ 2\Re\left(\dfrac{\zeta_3^j \log(N(\mathfrak{p}))}{N(\mathfrak{p})^\sigma - \zeta_3^j}\right) & \text{in (Case 2)}. \end{cases}$$

Moreover, the density function M_σ can be constructed as the inverse Fourier transform of the characteristic function $\varphi_{F_\sigma}(y)$, which in (Case 1) is given by

$$\varphi_{F_\sigma}(y) = \exp(-2yi\log(1-3^{-\sigma})) \prod_{\mathfrak{p}\nmid\langle 3\rangle}\left(\frac{1}{N(\mathfrak{p})+1} + \frac{1}{3}\frac{N(\mathfrak{p})}{N(\mathfrak{p})+1}\sum_{j=0}^{2}\exp\left(-2yi\log\left|1-\frac{\zeta_3^j}{N(\mathfrak{p})^\sigma}\right|\right)\right),$$

and in (Case 2) is given by

$$\varphi_{F_s}(y) = \exp\left(-2yi\Re\frac{\log(3)}{3^\sigma - 1}\right)\prod_{\mathfrak{p}\nmid\langle 3\rangle}\left(\frac{1}{N(\mathfrak{p})+1} + \frac{1}{3}\frac{N(\mathfrak{p})}{N(\mathfrak{p})+1}\sum_{j=0}^{2}\exp\left(-2yi\right.\right.$$
$$\left.\left.\cdot\,\Re\left(\frac{\zeta_3^j\log(N(\mathfrak{p}))}{N(\mathfrak{p})^\sigma - \zeta_3^j}\right)\right)\right).$$

As an application of the above theorem note that according to the class number formula

$$\mathcal{L}_c(1) = \frac{(2\pi)^2\sqrt{3}h_cR_c}{\sqrt{|D_c|}}$$

The value $\mathcal{L}_c(1)$ has some arithmetic significance. Here, h_c, R_c and $D_c = (-3)^5(N(c))^2$ are respectively the class number, the regulator, and the discriminant of the cubic extension $K_c = k(c^{1/3})$ (see [7], page 427] for more explanation). On the other hand by the Brauer-Siegel theorem we have $\log(h_cR_c) \sim \log|D_c|^{1/2}$, whenever $N(c) \to \infty$ (Note that the number fields K_c all have a fixed degree (namely 6) over $\mathbb{Q}$).

Corollary 5 *Let* $E(c) = \log(h_cR_c) - \log|D|^{1/2}$. *Then*

$$\lim_{Y\to\infty}\frac{1}{\mathcal{N}(Y)}\#\{c \in C : N(c) \le Y \text{and } E(c) \le z\} = \int_{-\infty}^{z+\log(4\sqrt{3}\pi^2)} M_1(t)dt,$$

where $M_1(t)$ *is the smooth function described in Theorem 4 (Case 1) for* $\sigma = 1$.

As another application note that the Euler-Kronecker constant of a number field K is defined by the relation

$$\gamma_K = \lim_{s\to 1}\left(\frac{\zeta_K'(s)}{\zeta_K} + \frac{1}{s-1}\right).$$

From (2) We concluded that $\dfrac{L_c'(1)}{L_c(1)} = \gamma_{K_c} - \gamma_k$. Thus, we get the following corollary of Theorem 4 (Case 2), since γ_k is fixed.

Corollary 6 *There exists a smooth function $M_1(t)$ (as described in Theorem 4 (Case 2) for $\sigma = 1$) such that*

$$\lim_{Y\to\infty} \frac{1}{\mathcal{N}(Y)} \#\{c \in C : N(c) \leq Y \text{and } \gamma_{K_c} \leq z\} = \int_{-\infty}^{z-\gamma_k} M_1(t)dt.$$

References

[1] S. Chowla and p. Erdős, *A theorem on the distribution of the values of L -function*. Indian Math. Soc. (N.S.), 15:1118–1951.

[2] P. D. T. A. Elliott, *The distribution of the quadratic class number, Litovsk*. Mat. Sb., 10:189–197, 1970.

[3] P. D. T. A. Elliott, *On the distribution of the values of Dirichlet L-series in the half-plane $\sigma \geq \frac{1}{2}$*, Nederl. Akad.Wetensch. Proc. Ser. A 74=Indag. Math., 33: 222–234, 1971.

[4] P. D. T. A. Elliott, *On the distribution of $arg L(s, \chi)$ in the half-plane $\sigma \geq \frac{1}{2}$* , Acta Arith., 20: 155–169, 1972.

[5] P. D. T. A. Elliott, *On the distribution of the values of quadratic L-series in the half-plane $\sigma \geq \frac{1}{2}$*, Invent. Math., 21: 319–338, 1973.

[6] Mariam Mourtada and V. Kumar Murty, Distribution of values of $L'/L(\sigma, \chi_D)$, Mosc. Math. J. 15 (2015), no. 3, 497–509, 605

[7] Honggang Xia, On zeros of cubic L-functions, J. Number Theory 124 (2007), no. 2, 415–428.

Andam Mustafa
Dipartimento di Matematica e Fisica
Università Roma Tre
Largo San Leonardo Murialdo,1.
email: andam.mustafa@gmail.com

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 4, *Number* 1, *March* 2019, *pages* 73-81

Adriana Salerno

Arithmetic, Hypergeometric Functions, and Mirror Symmetry

Written by Marine Rougnant

The talk is based on joint work with Tyler Kelly, Charles Doran, Steven Sperber, Ursula Whitcher and John Voight.

1 Motivation : quartics

Everything starts with an observation. Consider the five following quartics in $\mathbb{P}^3$:

Family	Equation
F_4 (Fermat/Dwork)	$x_0^4 + x_1^4 + x_2^4 + x_3^4$
F_2L_2	$x_0^4 + x_1^4 + x_2^3x_3 + x_3^3x_2$
F_1L_3 (Klein-Mukai)	$x_0^4 + x_1^3x_2 + x_2^3x_3 + x_3^3x_1$
L_2L_2	$x_0^3x_1 + x_1^3x_0 + x_2^3x_3 + x_3^3x_2$
L_4	$x_0^3x_1 + x_1^3x_2 + x_2^3x_3 + x_3^3x_0$

These quartics are not isomorphic : they have very different geometry. Let's have a look at the points where they vanish over finite fields. We count experimentally the number $\#X(\mathbb{F}_p)$ of $\mathbb{F}_p$-rational points of each quartic for several primes p.

p	F_4	F_2L_2	F_1L_3	L_2L_2	L_4
5	0	20	30	80	40
7	64	50	64	64	78
11	144	122	144	144	254
13	128	180	206	336	232
17	600	328	294	600	328
19	400	362	400	400	438
23	576	530	576	576	622
29	768	884	1116	1232	1000
31	1024	962	1024	1024	1334
37	1152	1300	1374	1744	1448

We remark that, for a fixed prime number p, all the values of the corresponding rows are equal (mod p).

To have a better idea of the phenomenon, we can consider pencils of quartics, adding to each equation a deforming term $-4\psi x_0x_1x_2x_3$. We can then count points over $\mathbb{F}_p$ on the pencil $X_{\diamond,\psi}$ of the family $\diamond$ for $0 \leqslant \psi < p$. We observe that, for a given p and for each parameter ψ, the point counts on $X_{\diamond,\psi}$ agree (mod p).

This equality holds for every p : these five quartics have different equations, different geometry but there is, arithmetically, something consistant.

2 Zeta functions

The number of rational points of an algebraic variety $X/\mathbb{F}_q$ over the finite fields with $q = p^s$ elements can be measured by looking at its Zeta function. We define the Zeta function of X as the formal power series:

$$Z(X/\mathbb{F}_q, T) = \exp\left(\sum_{s=1}^{\infty} N_s(X)\frac{T^s}{s}\right) \in \mathbb{Q}[\![T]\!],$$

where $N_s(X) := \#X(\mathbb{F}_{q^s})$ denotes the number of F_{q^s}-rational points on X.

The Weil conjectures, proven by Dwork and Deligne, state that the Zeta function of an algebraic variety X is indeed a rational function. If we denote by n the dimension of X, we can factorize $Z(X/\mathbb{F}_q, T)$ using polynomials with integer coefficients :

$$Z(X/\mathbb{F}_p, T) = \frac{\prod_{j=1}^{n} P_{2j-1}(T)}{\prod_{j=0}^{n} P_{2j}(T)},$$

where $P_0(T) = 1 - T$, $P_{2n}(T) = 1 - p^n T$ and $\deg P_j(T) = b_j = \dim H^j_{dR}(X)$ for all $1 \leqslant j \leqslant 2n - 1$.

In the particular case of smooth projective hypersurfaces in $\mathbb{P}^n$, it takes the following form :

$$Z(X, T) = \frac{P_X(T)^{(-1)^n}}{(1 - T)(1 - qT) \dots (1 - q^{n-1}T)}, P_X(T) \in \mathbb{Q}[T],$$

which gives for smooth quartics :

$$Z(X/\mathbb{F}_p, T) = \frac{P_X(T)^{-1}}{(1 - T)(1 - pT)(1 - p^2T)}.$$

Thus, the Zeta function of a smooth quartic is totally determinated by its numerator $P_X(T)$.

According to the definition of $Z(X/\mathbb{F}_p, T)$ and to the first observations that we made on the numbers of $\mathbb{F}_p$-rational points, we can expect the numerators $P_X(T)$ of the Zeta functions to have some common divisors in our previous examples. Using Edgar Costa's code, we compute the polynomial $P_{X_{\diamond,\psi}}(T)$ for $p = 41$ and $0 \leqslant \psi \leqslant 40$: we can observe shared quadratic factors, which are in fact parts of shared cubic factors, and we can predict the sructure of the other factors. The array below gives the obtained polynomials for some values of the parameters ψ and $\diamond$.

ψ	$\diamond$	$P_{X_{\diamond,\psi}}(T)$
0	F_4	$(1-41T)^{19}(1-18T+41^2T^2)$
	F_2L_2	$(1-41T)^{11}(1+41T)^8(1-18T+41^2T^2)$
	L_2L_2	$(1-41T)^{19}(1-18T+41^2T^2)$
2, 18, 23, 39	F_4	$(1-41T)^3(1+41T)^{16}(1-50T+41^2T^2)$
	F_2L_2	$(1-41T)^{11}(1+41T)^8(1-50T+41^2T^2)$
	L_2L_2	$(1-41T)^{11}(1+41T)^8(1-50T+41^2T^2)$
3, 14, 27, 38	F_4	$(1-41T)^{19}(1+78T+41^2T^2)$
	F_2L_2	$(1-41T)^{19}(1+78T+41^2T^2)$
	L_2L_2	$(1-41T)^{15}(1+41T)^4(1+78T+41^2T^2)$

3 Mirror symmetry

The five quartics that we take as examples are Calabi-Yau manifold. These structures are essential for physicists. Indeed, in string theory the results need to be transposed from a space in high dimension (where the superstrings are defined) to a realistic 4-dimension space. The remaining dimensions are "hidden" in a Calabi-Yau manifold.

For the string theory to work, they need two Calabi-Yau manifolds giving the same observable physics ; in this model to describe the universe, Calabi-Yau manifolds appear in pairs. This way of coupling manifolds is called Mirror symmetry.

The arithmetic patterns that we observe are a consequence of mirror symmetry.

3.1 Invertible polynomials

We need a construction of the swapping of properties in the "duality" induced by mirror symmetry. It can be done associating to each Calabi-Yau manifold a certain matrix.

We call invertible polynomial any polynomial of the form

$$F_A = \sum_{i=0}^{n} \prod_{j=0}^{n} x_j^{a_{ij}} \in \mathbb{Z}[x_0, \ldots, x_n],$$

where the matrix of exponents $A = (a_{ij})_{i,j}$ is an $(n+1) \times (n+1)$ matrix with nonnegative integer entries such that :

- A is invertible,
- F_A is quasi-homogeneous : there exist $r_0, \ldots, r_n \in \mathbb{N}$ and $d \in \mathbb{Z}$ such that $\sum_{j=0}^{n} r_j a_{ij} = d$,
- the function $F_A : \mathbb{C}^{n+1} \to \mathbb{C}$ has exactly one singular point at the origin.

An invertible polynomial defines a hypersurface X_A in the weighted projective space $W\mathbb{P}^n(r_0, \ldots, r_n)$. When F_A is invertible and homogeneous of degree $d = n + 1$, this hypersurface is a Calabi-Yau manifold.

If F_A is an invertible polynomial, so is F_{A^T}, where A^T is the transpose matrix of A. There exist nonnegative integral weights $q_0, \ldots, q_n$ so that $gcd(q_0, \ldots, q_n) = 1$ and $F_{A^T} = 0$ defines a hypersurface X_{A^T} in the weighted-projective space $W\mathbb{P}^n(q_0, \ldots, q_n)$. The integers $q_0, \ldots, q_n$ are called dual weights of F_A. We denote by $d^T = \sum_i q_i$ their sum.

♣	Equation	A	Dual weight	d^T
C_2F_2	$x_0^3x_1 + x_1^4 + x_2^4 + x_3^4$	$\begin{pmatrix} 3 & 1 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 4 \end{pmatrix}$	$(4, 2, 3, 3)$	12
C_2L_2	$x_0^3x_1 + x_1^4 + x_2^3x_3 + x_3^3x_2$	$\begin{pmatrix} 3 & 1 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 3 & 1 \\ 0 & 0 & 1 & 3 \end{pmatrix}$	$(4, 2, 3, 3)$	12

$\diamond$	Equation	A	Dual weight	d^T
F_4	$x_0^4 + x_1^4 + x_2^4 + x_3^4$	$\begin{pmatrix} 4 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 4 \end{pmatrix}$	$(1, 1, 1, 1)$	4
F_2L_2	$x_0^4 + x_1^4 + x_2^3x_3 + x_3^3x_2$	$\begin{pmatrix} 4 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 3 & 1 \\ 0 & 0 & 1 & 3 \end{pmatrix}$	$(1, 1, 1, 1)$	4
F_1L_3	$x_0^4 + x_1^3x_2 + x_2^3x_3 + x_3^3x_1$	$\begin{pmatrix} 4 & 0 & 0 & 0 \\ 0 & 3 & 1 & 0 \\ 0 & 0 & 3 & 1 \\ 0 & 1 & 0 & 3 \end{pmatrix}$	$(1, 1, 1, 1)$	4
L_2L_2	$x_0^3x_1 + x_1^3x_0 + x_2^3x_3 + x_3^3x_2$	$\begin{pmatrix} 3 & 1 & 0 & 0 \\ 1 & 3 & 0 & 0 \\ 0 & 0 & 3 & 1 \\ 0 & 0 & 1 & 3 \end{pmatrix}$	$(1, 1, 1, 1)$	4
L_4	$x_0^3x_1 + x_1^3x_2 + x_2^3x_3 + x_3^3x_0$	$\begin{pmatrix} 3 & 1 & 0 & 0 \\ 0 & 3 & 1 & 0 \\ 0 & 0 & 3 & 1 \\ 1 & 0 & 0 & 3 \end{pmatrix}$	$(1, 1, 1, 1)$	4

All that will follow can be extended to the pencil of hypersurfaces described by $F_A - d^T\psi x_0 \dots x_n = 0$.

3.2 Group action

The torus $(\mathbb{C}^*)^n$ acts coordinate-wise on $\mathbb{P}^n$, and therefore it acts on every Calabi-Yau manifold X_A given by an invertible polynomial F_A. Let fix notations for four remarkable groups :

- $SL(F_A)$, the subgroup of the torus that acts symplectically on X_A (fixes the holomorphic $n-1$-form),
- J_{F_A}, the subgroup of $SL(F_A)$ that acts trivially on X_A,
- $G = SL(F_A)/J_{F_A}$,
- $Z_{A,G} = X_A/G$.

3.3 Berglund-Hubsch-Krawitz mirror symmetry

Mirror symmetry depends on the transpose of the matrix A and on the group action. We start with a manifold X_A, corresponding to a

matrix A. Consider the transpose polynomial F_{A^T}. We saw that X_{A^T} is a Calabi-Yau manifold ; denote by G^T the quotient $SL(F_{A^T})/J(F_{A^T})$ defined by the action of the torus $(\mathbb{C}^*)^n$ on X_A. We obtain a dual orbifold $Z_{A^T,G^T} = X_{A^T}/G^T$, called Berglund-Hubsch-Krawitz (BHK) mirror of the orbifold $Z_{A,G}$.

BHK duality is a true duality: the mirror of the mirror yields the original orbifold.

4 Arithmetic applications of BHK mirror symmetry

We saw that the BHK mirror symmetry gives a duality relation between orbifolds. This duality has arithmetic consequences, in particular on Zeta functions of Calabi-Yau manifolds.

Let's recall that our smooth quartics have a Zeta function of the form

$$Z(X/\mathbb{F}_p, T) = \frac{P_X(T)^{-1}}{(1-T)(1-pT)(1-p^2T)}.$$

From our observations, we expect the polynomials $P_{X_{A,\psi}}(T)$ and $P_{X_{B,\psi}}(T)$ of two different pencils of the $\diamond$-family to share a common factor. The following theorem confirms this prediction and gives lower and upper bounds of the degree of this common factor.

Theorem. *(DKSSVW) Let $X_{A,\psi}$ and $X_{B,\psi}$ be invertible pencils of Calabi-Yau $(n-1)$-folds in $\mathbb{P}^n$. Suppose A and B have the same dual weights $(q_0, \ldots, q_n)$. Then for each $\psi \in \mathbb{F}_q$ such that $\gcd(q, (n+1)d^T) = 1$ and the fibers $X_{A,\psi}$ and $X_{B,\psi}$ are nondegenerate and smooth, the polynomials $P_{X_{A,\psi}}(T)$ and $P_{X_{B,\psi}}(T)$ have a common factor $R_\psi(T) \in \mathbb{Q}[T]$ with*

$$\deg R_\psi(T) \geqslant D(q_0, \ldots, q_n).$$

Furthermore, $\deg R_\psi(T) \leqslant \dim_{\mathbb{C}} H^{n-1}_{\text{prim}}(X_{A,\psi}, \mathbb{C})^{SL(F_A)}$.

$\diamond$	Equation	$SL(F_A)/J_{F_A}$
F_4	$x_0^4 + x_1^4 + x_2^4 + x_3^4 - 4\psi x_0x_1x_2x_3$	$(\mathbb{Z}/4\mathbb{Z})^2$
F_2L_2	$x_0^4 + x_1^4 + x_2^3x_3 + x_3^3x_2 - 4\psi x_0x_1x_2x_3$	$\mathbb{Z}/8\mathbb{Z}$
F_1L_3	$x_0^4 + x_1^3x_2 + x_2^3x_3 + x_3^3x_1 - 4\psi x_0x_1x_2x_3$	$\mathbb{Z}/7\mathbb{Z}$
L_2L_2	$x_0^3x_1 + x_1^3x_0 + x_2^3x_3 + x_3^3x_2 - 4\psi x_0x_1x_2x_3$	$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
L_4	$x_0^3x_1 + x_1^3x_2 + x_2^3x_3 + x_3^3x_0 - 4\psi x_0x_1x_2x_3$	$\mathbb{Z}/5\mathbb{Z}$
$\clubsuit$	Equation	$SL(F_A)/J_{F_A}$
C_2F_2	$x_0^3x_1 + x_1^4 + x_2^4 + x_3^4 - 12\psi x_0x_1x_2x_3$	$\mathbb{Z}/4\mathbb{Z}$
C_2L_2	$x_0^3x_1 + x_1^4 + x_2^3x_3 + x_3^3x_2 - 12\psi x_0x_1x_2x_3$	$\mathbb{Z}/2\mathbb{Z}$

The five first pencils of quartics have the same dual weights $(1, 1, 1, 1)$. Their polynomials $P_{X,\psi}$ have a common factor $R_\psi(T)$ of degree 3 according the theorem. The two pencils of the $\clubsuit$-family have dual weights $(4, 2, 3, 3)$. They also have a common factor, but in this case, we cannot determine its degree : the theorem juts says that $6 \leqslant \deg R_\psi(T) \leqslant 7$.

From now, for any invertible pencil of Calabi-Yau $(n-1)$-folds in $\mathbb{P}^n$, we can write

$$P_{X,\psi}(T) = Q_{X,\psi}(T)R_\psi(T),$$

where $R_\psi(T)$ uniquely depends on the family of pencils. Next step in the understanding of Zeta functions is to determine $Q_{X,\psi}(T)$. Finally, using hypergeometric motives, we can show :

Theorem. *(DKSSVW) The polynomials $Q_{\diamond,\psi,q}(T)$ factor over $\mathbb{Z}[T]$ according to the following table :*

Family	Factorisation	Hypothesis	r_0
F_4	$(\deg 2)^3(\deg 1)^{12}$	$q \equiv 1 (\mathrm{mod}\ 4)$	2
F_1L_3	$(\deg 6)^3$	$q \equiv \pm 1 (\mathrm{mod}\ 7)$	18
F_2L_2	$(\deg 2)^1(\deg 1)^2(\deg 2)^4(\deg 1)^6$	$q \equiv 1 (\mathrm{mod}\ 8)$	16
L_2L_2	$(\deg 2)^1(\deg 4)^2(\deg 2)^4$	$q \equiv 1 (\mathrm{mod}\ 4)$	20
L_4	$(\deg 4)^4(\deg 1)^2$	$q \equiv 1 (\mathrm{mod}\ 5)$	4

Moreover, if $q = p^r$ with $r_0 | r$ then $Q_{\diamond,\psi,q}(T) = (1 - qT)^{18}$.

References

[1] C. F. Doran, T. L. Kelly, A. Salerno, S. Sperber, J. Voight, U. Whitcher, *Zeta functions of alternate mirror Calabi-Yau families*.

[2] P. Candelas, X. C. de la Ossa, F. Rodriguez Villegas, *Calabi-Yau manifolds over finite fields*. Calabi-Yau varieties and mirror symmetry, 121–157, Toronto, 2001.

Marine Rougnant
Laboratoire de Mathématiques de Besançon
Université de Bourgogne Franche-Comté
16 route de Gray
25030 Besançon Cedex, France.
email: marine.rougnant@univ-fcomte.fr

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 4, *Number* 1, *March* 2019, *pages* 83-89

Alberto Perelli

Explicit formulae for averages of Goldbach representations

Written by Remis Tonon

1 Introduction

Surely the most famous explicit formula in analytic number theory is the one for the second Chebyshev function, which was proposed by Riemann in his memoir and proved in 1895 by von Mangoldt:

$$\psi(x) = x - \sum_{\rho} \frac{x^{\rho}}{\rho} - \frac{\zeta'}{\zeta}(0) - \frac{1}{2}\log\left(1 - \frac{1}{x^2}\right).$$

Since then, several explicit formulae were proved for different arithmetic functions or their means. Hence, one may wish to know if a similar formula exists for the function that counts the number of points with prime coordinates in a triangle, that is

$$\sharp\{(p, p') : p + p' \le N,\ p \text{ and } p' \text{ prime}\} = \sum_{n \le N} \sum_{\substack{p,\, p' \text{ prime} \\ p+p'=n}} 1.$$

As it is clear by the last way of writing it, this quantity can be interpreted also as the mean of the number of representations of the integers $n \le N$ as the sum of two primes (the Goldbach representations). As customary,

in order to apply analytic methods, instead of counting just primes one is led to consider the sum extended to all the integers weighted with the von Mangoldt function, so obtaining

$$G_0(N) := \sum_{n\le N}{}' R(n), \quad \text{where } R(n) := \sum_{m+m'=n} \Lambda(m)\Lambda(m').$$

The notation means that, if $N \in \mathbb{N}$, $R(N)/2$ must be subtracted from the first sum. By the classical results on the Goldbach problem, it is expected that $R(n) \sim n\mathfrak{S}(n)$, where $\mathfrak{S}(n)$ is the well known singular series; since this has mean 1, it should be true also that $G_0(N) \sim N^2/2$.

2 Some history of the problem

The first step towards an explicit formula was to prove not only the just mentioned asymptotic behaviour of $G_0(N)$, but also to find a second term in addition to the main one, so obtaining the formula

$$G_0(N) = \frac{1}{2}N^2 - 2\sum_{\rho} \frac{N^{\rho+1}}{\rho(\rho+1)} + E(N),$$

where, as a remark, we note that the sum is absolutely convergent. This was achieved, under the Riemann hypothesis, by:

- Fujii [3] in 1991, with $E(n) \ll (N\log N)^{4/3}$;
- Bhowmik & Schlage-Puchta [1] in 2010, with $E(n) \ll N\log^5 N$;
- Languasco & Zaccagnini [5] in 2012, with $E(n) \ll N\log^3 N$.

As an interesting and natural extension, Languasco and Zaccagnini were led to study the function

$$G_k(N) = \frac{1}{\Gamma(k+1)} \sum_{n<N} R(n)\left(1-\frac{n}{N}\right)^k \quad \text{for } k \ge 0,$$

which is the Cesàro-Riesz mean for the number of representations defined above and which is equal to the previous function for $k = 0$ and $N \notin \mathbb{N}$. In [6], they proved that unconditionally, for $k > 1$, it holds

$$G_k(N) = \frac{N^2}{\Gamma(k+3)} - 2A_k(N) + B_k(N) + O(N),$$

where

$$A_k(N) = \sum_{\rho} \frac{\Gamma(\rho)}{\Gamma(\rho+k+2)} N^{\rho+1},$$
$$B_k(N) = \sum_{\rho} \sum_{\rho'} \frac{\Gamma(\rho)\Gamma(\rho')}{\Gamma(\rho+\rho'+k+1)} N^{\rho+\rho'}.$$

For $k = 1$, Goldston and Young [4] were able to obtain a similar result under the Riemann hypothesis.

3 A new approach

All the mentioned results were obtained by using the circle method. In their recent work, instead, Brüdern, Kaczorowski and Perelli [2] have dealt with the problem in a different way and have managed to obtain a formula which is fully explicit.

Their first idea consists in rewriting $G_k(N)$ by means of the simple, but technically critical observation that

$$1 - \frac{m+n}{N} = \left(1 - \frac{n}{N-m}\right)\left(1 - \frac{m}{N}\right),$$

so that

$$\begin{aligned} G_k(N) &= \frac{1}{\Gamma(k+1)} \sum_{m<N} \Lambda(m) \left(1 - \frac{m}{N}\right)^k \sum_{n<N-m} \Lambda(n) \left(1 - \frac{n}{N-m}\right)^k \\ &= \frac{1}{(2\pi \mathrm{i})^2} \int_{(2)} \int_{(2)} \frac{\zeta'}{\zeta}(w) \frac{\zeta'}{\zeta}(s) \frac{\Gamma(w)\Gamma(s)}{\Gamma(w+s+k+1)} N^{w+s} \, ds \, dw, \end{aligned}$$

where to obtain the second equality a double Mellin transform has been performed. As usual, one would like to shift the real part of the lines of integration to $-\infty$ and then evaluate the residues; unfortunately, this is possible only up to a certain point, because there are serious problems of convergence associated to the trivial zeros from some value on. To understand the role of this operation and the importance of trying to move the lines as to the left as possible in the complex plane, we remark that, for example, shifting the lines to 0 (in real parts) gives the already mentioned result by Languasco and Zaccagnini [6].

Hence, the three authors show that the s-integral can be shifted from $\Re s = 2$ to $\Re s = -1/2$. In this operation, two functions arise, namely

$$T_N(w) = -\frac{1}{2\pi \mathrm{i}} \int_{\left(-\frac{1}{2}\right)} \frac{\zeta'}{\zeta}(s)\, \frac{\Gamma(s)}{\Gamma(w+s+1)}\, N^s\, ds,$$
$$Z_N(w) = \sum_{\rho} \frac{\Gamma(\rho)}{\Gamma(\rho+w+1)}\, N^{\rho},$$

where either the integral and the sum are are absolutely and compactly convergent in $w > 0$, and so they are both holomorphic there. A key fact, which is proved in Proposition 1 and 2 of [2], is that, for $N \geq 4$, these two functions extend to entire functions with controlled growing ratio.

To be more precise, there exists a real number K such that, for any δ with $0 < \delta < 1$ and any $w = u + \mathrm{i}v$ such that $|w + m| > \delta$ for all integers $m \geq 1$, we have

$$T_N(w) \leq K\, \frac{2^{|u|} \log(|w|+2)}{\delta\, |\Gamma(w+1)|},$$
$$Z_N(w) \leq \frac{K}{\delta\, |\Gamma(w+1)|} \cdot \begin{cases} N^{|u|+1} + 2^{|u|} \log(|w|+2) & \text{if } u \in \mathbb{R}, \\ N^{|u|} \log N + 2^{|u|} \log |w| & \text{if } u \leq -3/2. \end{cases}$$

Using this result, one can now shift the w-integration from $\Re w = 2$ to $\Re w = -M$, where M can vary, and even go to infinity. In this way, the

following result, containing the announced completely explicit formula, can be reached.

Theorem 1 *Let us define*

$$\Sigma_\Gamma(N,k) = -\sum_{\nu=1}^{\infty} \operatorname*{res}_{w=-\nu} \frac{\zeta'}{\zeta}(w)\Gamma(w)\frac{N^w}{\Gamma(w+k+1)},$$

$$\Sigma_Z(N,k) = -\sum_{\nu=1}^{\infty} \operatorname*{res}_{w=-\nu} \frac{\zeta'}{\zeta}(w)\Gamma(w)Z_N(w+k)N^w,$$

$$\Sigma_T(N,k) = -\sum_{\nu=1}^{\infty} \operatorname*{res}_{w=-\nu} \frac{\zeta'}{\zeta}(w)\Gamma(w)T_N(w+k)N^w.$$

Then, for N integer, $N \geq 4$, and $k > 0$, we have

$$\begin{aligned} G_k(N) = {} & \frac{N^2}{\Gamma(k+3)} - 2NZ_N(k+1) + \sum_\rho \Gamma(\rho)Z_N(\rho+k)N^\rho \\ & - 2\frac{\zeta'}{\zeta}(0)\frac{N}{\Gamma(k+2)} + 2\frac{\zeta'}{\zeta}(0)Z_N(k) + NT_N(k+1) \\ & + \left(\frac{\zeta'}{\zeta}(0)\right)^2 \frac{1}{\Gamma(k+1)} - \sum_\rho \Gamma(\rho)T_N(\rho+k)N^\rho - \frac{\zeta'}{\zeta}(0)T_N(k) \\ & + N\Sigma_\Gamma(N,k+1) - \Sigma_Z(N,k) - \frac{\zeta'}{\zeta}(0)\Sigma_\Gamma(N,k) + \Sigma_T(N,k), \end{aligned}$$

where the sums defined above and the ones over nontrivial zeros of $\zeta(s)$ are absolutely convergent.

To conclude, we make some final remarks.

- The series which define $\Sigma_\Gamma(N,k)$ and $\Sigma_T(N,k)$ are actually asymptotic expansions: this means that, when considering the series truncated at $\nu = M \geq 2$, a sharp error term is obtained, which is roughly $O\left(N^{-M-1}\right)$. This does not hold for $\Sigma_Z(N,k)$: for the

tail of its defining series one can only get an error term which is $O\left(N^{-k+\varepsilon}\right)$ for every $\varepsilon > 0$, which is actually an overall error term.

- If one restricts to $k \geq 1/2$, one can recover the same main terms as in Languasco and Zaccagnini [6].
- Following this multiplicative approach, which avoids the use of the circle method, even without the main propositions about the analytic continuation an explicit formula can be reached with an overall error term which is $o(1)$.

References

[1] G. Bhowmik and J.-C. Schlage-Puchta, *M*ean representation number of integers as the sum of primes, Nagoya Math. J., 200 (2010), pp. 27–33.

[2] J. Brüdern, J. Kaczorowski, and A. Perelli, *Explicit formulae for averages of Goldbach representations*, to appear in Trans. Amer. Math. Soc.

[3] A. Fujii, *An additive problem of prime numbers. II*, Proc. Japan Acad. Ser. A Math. Sci., 67 (1991), pp. 248–252.

[4] D. A. Goldston and L. Yang, *The average number of Goldbach representations*, arXiv:1601.06902 (2016).

[5] A. Languasco and A. Zaccagnini, *T*he number of Goldbach representations of an integer, Proc. Amer. Math. Soc., 140 (2012), pp. 795–804.

[6] A. Languasco and A. Zaccagnini, *A* Cesàro average of Goldbach numbers, Forum Math., 27 (2015), pp. 1945–1960.

Remis Tonon
Dipartimento di Scienze Matematiche, Fisiche e Informatiche
Università degli Studi di Parma
Parco Area delle Scienze, 53/A
43124 Parma, Italy.
email: remis.tonon@unimore.it

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 4, *Number* 1, *March* 2019, *pages* 91-100

Ade Irma Suriajaya

Zeros of the derivatives of the Riemann zeta function and Dirichlet L-functions

Written by Giamila Zaghloul

1 Introduction

The *Riemann zeta function* $\zeta(s)$ is defined as the Dirichlet series

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

in the half-plane $\Re(s) > 1$ and it is an analytic function on $\mathbb{C} \setminus \{1\}$. Given a primitive Dirichlet character $\chi \pmod q$, with $q > 1$, the Dirichlet L-function $L(s, \chi)$ is entire and satisfies

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} \quad \text{for} \quad \Re(s) > 0.$$

It is well-known that the negative even integers are the so-called *trivial zeros* of the Riemann zeta function, while the set

$$Z := \{\rho \in \mathbb{C} \mid \zeta(s) = 0, \rho \notin -2\mathbb{N}_0\}$$

is the set of all *non-trivial zeros* of $\zeta(s)$. These zeros are non-real and they are all located in the right half-plane $\Re(s) > 0$. The Riemann hypothesis (RH) states that, for any $\rho \in Z$, $\Re(\rho) = \frac{1}{2}$.

For a primitive character χ modulo $q \geq 1$, let $\kappa \in \{0, 1\}$ be determined by $\chi(-1) = (-1)^\kappa$. The set of the *trivial zeros* of $L(s, \chi)$ is $\{-\kappa, -2 - \kappa, -4 - \kappa, \dots\}$, while the set of the *non-trivial zeros* is

$$Z(\chi) := \{\rho \in \mathbb{C} \mid L(\rho, \chi) = 0, \rho \neq -2l - \kappa, \forall l \in \mathbb{N}\}.$$

As for the Riemann zeta function, these non-trivial zeros have positive real part, but they are not necessarily non-real. The Generalized Riemann Hypothesis (GRH) states that

$$\Re(\rho) = \frac{1}{2} \quad \text{for any} \rho \in Z \cup Z(\chi).$$

There is an equivalence for RH in terms of zeros of the first derivative of the Riemann zeta function (cf. [8]).

Theorem 1 (Speiser) *The following statements are equivalent*

1. $\zeta(s) \neq 0$ *in* $0 < \Re(s) < \frac{1}{2}$
2. $\zeta'(s) \neq 0$ *in* $0 < \Re(s) < \frac{1}{2}$.

The result below (see [5]) is a sort of analytic analogue of Speiser's theorem. It basically states that $\zeta(s)$ and its first derivative have almost the same number of zeros in the considered region.

Theorem 2 (Levison and Montgomery) *Let $N^-(T)$ (and respectively $N_1^-(T)$) be the number of zeros of $\zeta(s)$ (resp. $\zeta'(s)$) in $\{\sigma + it \mid 0 < \sigma < 1/2, 0 < t < T\}$, counted with multiplicity. Then, for $T \geq 2$*

$$N^-(T) = N_1^-(T) + O(\log T),$$

where the implied constant is absolute.

Similar results can be proved for Dirichlet L-functions. Let $N^-(T,\chi)$ (and respectively $N_1^-(T,\chi)$) be the number of zeros of $L(s,\chi)$ (resp. $L'(s,\chi)$) in the region $\{\sigma+it \mid 0<\sigma<1/2, |t|<T\}$, counted with multiplicity. Moreover, let

$$m := \min\{n \geq 2 \mid \chi(n) \neq 0\},$$

i.e. m is the smallest prime number that does not divide n. Observe that $m = O(\log T)$. The following result holds ([2]).

Theorem 3 (Akatsuka and Suriajaya) *For $T \geq 2$*

$$N^-(T,\chi) = N_1^-(T,\chi) + O(m^{1/2}\log(qT)),$$

where the implied constant is absolute.

This allows to show a Speiser-type equivalence for GRH (again cf. [2]).

Theorem 4 (Akatsuka and Suriajaya) *Let $\kappa = 0$ and $q \geq 216$. Then the following statements are equivalent*

(i) $L(s,\chi) \neq 0$ *in* $0 < \Re(s) < \frac{1}{2}$.

(ii) $L'(s,\chi)$ *has a unique zero in* $0 < \Re(s) < \frac{1}{2}$.

Let $\kappa = 1$ and $q \geq 23$. Then the following statements are equivalent

(i) $L(s,\chi) \neq 0$ *in* $0 < \Re(s) < \frac{1}{2}$.

(ii) $L'(s,\chi)$ *has no zeros in* $0 < \Re(s) < \frac{1}{2}$.

Remark 1 *The unique zero of the derivative for $\kappa = 0$ is the zero which corresponds to the trivial zero of $L(s,\chi)$ at $s = 0$.*

2 Zeros of derivatives of the Riemann zeta function

As for the Riemann zeta function, *non-trivial zeros* of $\zeta^{(k)}(s)$ are non-real zeros. As an upper bound for the real part of the zeros ρ of $\zeta^{(k)}(s)$ one can consider $\Re(\rho) \leq \frac{7}{4}k + 2$, proved by Spira [9], even though this bound can be slightly improved.

Remark 2 *It is interesting to observe the distribution of non-trivial zeros of $\zeta(s)$, $\zeta'(s)$ and $\zeta''(s)$ (cf. [9, Fig. 1]). So far, all non-trivial zeros of $\zeta(s)$ lie on the line $\Re(s) = \frac{1}{2}$, while those of $\zeta'(s)$ and $\zeta''(s)$ move further and further to the right. Moreover, except for a pair of exceptional zeros of $\zeta''(s)$ in the left half-plane, the non-trivial zeros of the first and second derivative seem to appear always in pairs.*

Let now $N(T)$ (resp. $N_k(T)$) be the number of non-trivial zeros ρ of $\zeta(s)$ (resp. $\zeta^{(k)}(s)$), with $0 < \Im(\rho) < T$, counted with multiplicity. Then, von Mangoldt [12] and Berndt [3] respectively proved

$$N(T) = g(T) + O(\log T)$$
$$N_k(T) = h(T) + O(\log T)$$

where

$$g(T) := \frac{T}{2\pi}\log\frac{T}{2\pi} - \frac{T}{2\pi} \quad \text{and} \quad h(T) := \frac{T}{2\pi}\log\frac{T}{4\pi} - \frac{T}{2\pi}.$$

Under the Riemann hypothesis, the error terms can be improved to

$$O\left(\frac{\log T}{\log\log T}\right) \quad \text{and} \quad O\left(\frac{\log T}{(\log\log T)^{1/2}}\right)$$

respectively. The result for $\zeta(s)$ is due to Littlewood [6], for the first derivative to Akatsuka [1] and the extension to all $k \geq 2$ to Suriajaya [10]. It can be observed that the main term does not depend on k.
Assuming RH, Ge [4] showed that the error term can be improved to

$O\left(\frac{\log T}{\log\log T}\right)$ for the first derivative, while the same result for $k \geq 2$ is expected to hold but it is not proved.

Let now $\sum^{(k)}$ denote the sum over non-trivial zeros ρ of $\zeta^{(k)}(s)$, for $k \geq 0$, with $0 < \Im(\rho) < T$, counted with multiplicity and let

$$f_k(T) = \frac{kT}{2\pi}\log\log\frac{T}{2\pi} + \frac{T}{2\pi}\left(\frac{1}{2}\log 2 - k\log\log 2\right) - k\int_2^{\frac{T}{2\pi}} \frac{dt}{\log t}.$$

Since the zeros of $\zeta(s)$ are symmetric with respect to the critical line $\Re(s) = \frac{1}{2}$, one gets

$$\Sigma^{(0)}\left(\Re(s) - \frac{1}{2}\right) = 0.$$

On the other hand, for higher derivatives the zeros are no more symmetric. In [5], Levinson and Montgomery proved that

$$\Sigma^{(k)}\left(\Re(s) - \frac{1}{2}\right) = f_k(T) + O(\log T).$$

Under RH, the error term can be improved to $O((\log\log T)^2)$. This result is due to Akatsuka [1] for $k = 1$ and to Suriajaya [10] for $k \geq 2$.

3 Zeros of derivatives of Dirichlet L-functions

In [13], Yıldırım described a zero-free region for the derivatives of the Dirichlet L-functions.

Theorem 5 (Yıldırım) *For any $\epsilon > 0$, there exists a constant $K = K_{\epsilon,k}$ such that $L^{(k)}(s,\chi) \neq 0$ holds in*

$$\left\{\sigma + it \in \mathbb{C} \;\middle|\; \sigma > 1 + \frac{m}{2}\left(1 + \sqrt{1 + \frac{4k^2}{m\log m}}\right)\right\}$$
$$\cup \{\sigma + it \in \mathbb{C} || \sigma + it| > q^K, \sigma < -\epsilon, |t| > \epsilon\}.$$

He also classified the zeros of $L^{(k)}(s,\chi)$ in the following way:

- *trivial zeros*, located in $\{\sigma+it|\sigma\leq -q^K, |t|\leq\epsilon\}$.
- *vagrant zeros*, located in $\{\sigma+it||\sigma+it|\leq q^K, \sigma\leq -\epsilon\}$.
- *non-trivial zeros*, located in

$$\left\{\sigma+it\;\middle|\; -\epsilon<\sigma\leq 1+\frac{m}{2}\left(1+\sqrt{1+\frac{4k^2}{m\log m}}\right)\right\}.$$

Let now $N_k(T,\chi)$ be the number of non-trivial and vagrant zeros ρ of $L^{(k)}(s,\chi)$, with $|\Im(\rho)|\leq T$, counted with multiplicity.

Theorem 6 (Yıldırım) *For $T\geq 2$, we have*

$$N_k(T,\chi)=h(T,\chi)+O(q^K\log T),$$

where

$$h(T,\chi):=\frac{T}{\pi}\log\frac{qT}{2m\pi}-\frac{T}{\pi}.$$

Remark 3 *In this case, the error term is big in terms of the modulus q of the character χ, since K is big. Assuming GRH does not help to improve the error term in terms of q.*

4 Zeros of the first derivative $L'(s,\chi)$

In [2], Akatsuka and Suriajaya proved that there exist no vagrant zeros for the first derivative of a Dirichlet L-function. A zero-free region is described in the result below.

Theorem 7 (Akatsuka and Suriajaya) *Let χ be a primitive Dirichlet character modulo $q>1$. Then $L'(s,\chi)$ has no zeros in*

$$\left\{\sigma+it\;\middle|\;\sigma\leq 0, |t|\geq\frac{6}{\log q}\right\}\cup\left\{\sigma+it\;\middle|\;\sigma\leq -q^2, |t|\geq\frac{12}{\log|\sigma|}\right\}.$$

Remark 4 *The zero-free region can be extended to the line* $\Re(s) = \frac{1}{2}$ *under GRH, avoiding zeros of* $L(s, \chi)$.

Remark 5 *Except for a finite number of zeros, each zero of* $L'(s, \chi)$ *in* $\Re(s) \leq 0$ *corresponds to a trivial zero of* $L(s, \chi)$.

More precisely, the following result holds.

Theorem 8 (Akatsuka and Suriajaya) *For each* $j \in \mathbb{N}_0$*:*

- $L'(s, \chi)$ *has exactly a unique zero at*

$$-2j - \kappa + O\left(\frac{1}{\log(jq)}\right)$$

  in the strip $-2j - \kappa - 1 < \Re(s) < -2j - \kappa + 1$.

- $L'(s, \chi)$ *has no zeros on* $\Re(s) = -2j - \kappa + 1$.

1. *If* $\kappa = 0$ *and* $q \geq 7$*, then* $L'(s, \chi)$ *has no zeros in the strip* $-1 \leq \Re(s) \leq 0$.

2. *If* $\kappa = 1$ *and* $q \geq 23$*, then* $L'(s, \chi)$ *has a unique zero in the strip* $-2 \leq \Re(s) \leq 0$

Remark 6 *If the character is odd, the unique zero of* $L'(s, \chi)$ *corresponds to the trivial zero of* $L(s, \chi)$ *at* $s = -1$.

For the excluded characters, there is at most a finite number of zeros of $L'(s, \chi)$ in $-1 \leq \Re(s) \leq 0$ if the character is even and in $-2 \leq \Re(s) \leq 0$ if the character is odd. Then, except for a finite number of Dirichlet character, there is a one-to-one correspondence between the zeros of $L'(s, \chi)$ in $\Re(s) \leq 0$ and the trivial zeros of $L(s, \chi)$. Thus, the zeros in the left half-plane of $L'(s, \chi)$ can all be classified as trivial.

One can now focus on the non-trivial zeros in the right half-plane. In [7], Selberg proved that

$$N(T, \chi) = g(T, q) + O(\log(qT)),$$

where $N(T, \chi)$ is the number of zeros ρ of $L(s, \chi)$ with $\Re(\rho) > 0$ and $|\Im(\rho)| \leq T$, counted with multiplicity and

$$g(T, q) := \frac{T}{\pi} \log \frac{qT}{2\pi} - \frac{T}{\pi}.$$

He also improved the error term to $O\left(\frac{\log(qT)}{\log\log(qT)}\right)$ under GRH.

In the unconditional case, Akatsuka and Suriajaya [2] improved the error term to $O(m^{1/2} \log(qT))$ for the number of non-trivial zeros of $L'(s, \chi)$ in the right half-plane. Recalling that $m = O(\log q)$, notice that the error term is small.

Assuming GRH, Suriajaya [11] got an error term of the form

$$O\left(\log q + A(q, T) \frac{m^{1/2} \log(qT)}{\log\log(qT)} \right),$$

where $A(q, T)$ is a comparison factor

$$A(q, T) := \min \left\{ (\log\log(qT))^{1/2}, 1 + \frac{m^{1/2}}{\log\log(qT)} \right\}.$$

Another improvement to the error term, under GRH, was proved by Ge (2018). He got

$$O\left(\frac{\log(qT)}{\log\log(qT)} + \sqrt{m \log(2m) \log(qT)} \right).$$

Finally, as in the case of $\zeta(s)$ and its derivatives, one can consider the real part distribution of the zeros. Let $\sum^{(0)}$ and $\sum'$ denote the sum over the zeros ρ, with $\Re(\rho) > 0$ and $|\Im(\rho)| \leq T$, counted with multiplicity, of $L(s, \chi)$ and $L'(s, \chi)$ respectively. Then,

$$\Sigma^{(0)}\left(\Re(\rho) - \frac{1}{2} \right) = 0$$

and

$$\Sigma'\left(\Re(\rho) - \frac{1}{2} \right) = f_1(T, \chi) + O(m^{1/2} \log(qT)),$$

where

$$f_1(T,\chi) = \frac{T}{\pi}\log\log\frac{qT}{2\pi} + \frac{T}{\pi}\left(\frac{1}{2}\log m - \log\log m\right) - \frac{2}{q}\int_2^{\frac{qT}{2\pi}} \frac{dt}{\log t}.$$

This result was proved by Akatsuka and Suriajaya [2], while in [11] Suriajaya also proved that, under the generalized Riemann hypothesis, the error term can be improved to

$$O(m^{1/2}(\log\log(qT))^2 + m\log\log(qT) + m^{1/2}\log q).$$

References

[1] H. Akatsuka, *Conditional estimates for error terms related to the distribution of zeros of $\zeta'(s)$*, J. Number Theory 132 (2012), no. 10, 2242−2257.

[2] H. Akatsuka and A. I. Suriajaya, *Zeros of the first derivative of the Riemann zeta function*, J. Number Theory 184 (2018) 300−329.

[3] B. C. Berndt, *The number of zeros for $\zeta^{(k)}(s)$*, J. London Math. Soc. (2) 2 (1970) 577−580.

[4] F. Ge *The Number of Zeros of $\zeta'(s)$*, International Mathematics Research Notices (2017), no. 5, 1578−1588.

[5] N. Levinson and H. Montgomery, *Zeros of the derivative of the Riemann zeta- function*, Acta Math. 133 (1974) 49−65.

[6] J.E. Littlewood, *On the zeros of the Riemann zeta-function*, Proc. Camb. Philos. Soc. 22 (1924) 295−318.

[7] A. Selberg, *Contributions to the theory of Dirichlet's L-functions*, Skr. Norske Vid. Akad. Oslo. I (1946) 1−62.

[8] A. Speiser, *Geometrisches zur Riemannschen Zetafunktion*, Math. Ann. 110 (1935) 514-521.

[9] R. Spira, *Zero-free regions of* $\zeta^{(k)}(s)$, J. Lond. Math. Soc. 40 (1965) 677−682.

[10] A.I. Suriajaya, *On the zeros of the k-th derivative of the Riemann zeta function under the Riemann Hypothesis*, Funct. Approx. Comment. Math. 53 (2015), no. 1, 69−95.

[11] A.I. Suriajaya, *Two estimates on the distribution of zeros of the first derivative of Dirichlet L-functions under the generalized Riemann hypothesis*, Journal de Théorie des Nombres de Bordeaux Vol. 29 (2017), no. 2, 471−502.

[12] H.C.F. von Mangoldt, *Zur Verteilung der Nullstellen der Riemannschen Funktion* $\zeta(s)$, Math. Ann. 60 (1905) 1−19.

[13] C.Y. Yıldırım, *Zeros of derivatives of Dirichlet L-functions*, Turkish J. Math. 20 (1996) 521−534.

Giamila Zaghloul
Dipartimento di Matematica
Università degli Studi di Genova
via Dodecaneso 35
16246 Genova, Italia.
email: zaghloul@dima.unige.it

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 4, *Number* 1, *March* 2019, *pages* 101-114

Michel Waldschmidt

Representation of integers by cyclotomic binary forms

Editorial Committe

The homogeneous form $\Phi_n(X, Y)$ of degree $\varphi(n)$ which is associated with the cyclotomic polynomial $\phi_n(t)$ is dubbed a cyclotomic binary form. A positive integer $m \geq 1$ is said to be representable by a cyclotomic binary form if there exist integers n, x, y with $n \geq 3$ and $\max\{|x|, |y|\} \geq 2$ such that $\Phi_n(x, y) = m$. These definitions give rise to a number of questions that we are going to address.

This is a joint work with Čtienne Fouvry and Claude Levesque [FLW].

1 Cyclotomic polynomials

1.1 Definition

The sequence $(\phi_n(t))_{n\geq 1}$ can be defined by induction:

$$\phi_1(t) = t - 1, \qquad t^n - 1 = \prod_{d|n} \phi_d(t).$$

Hence,

$$\phi_n(t) = \frac{t^n - 1}{\prod\limits_{\substack{d \neq n \\ d|n}} \phi_d(t)}.$$

When p is prime, from

$$t^p - 1 = (t-1)(t^{p-1} + t^{p-2} + \cdots + t + 1) = \phi_1(t)\phi_p(t),$$

one deduces $\phi_p(t) = t^{p-1} + t^{p-2} + \cdots + t + 1$. For instance

$$\phi_2(t) = t + 1, \quad \phi_3(t) = t^2 + t + 1, \quad \phi_5(t) = t^4 + t^3 + t^2 + t + 1.$$

Further examples are

$$\phi_4(t) = \frac{t^4 - 1}{\phi_1(t)\phi_2(t)} = \frac{t^4 - 1}{t^2 - 1} = t^2 + 1 = \phi_2(t^2),$$

$$\phi_6(t) = \frac{t^6 - 1}{\phi_1(t)\phi_2(t)\phi_3(t)} = \frac{t^6 - 1}{(t+1)(t^3 - 1)} = \frac{t^3 + 1}{t + 1} = t^2 - t + 1 = \phi_3(-t).$$

The degree of $\phi_n(t)$ is $\varphi(n)$, where φ is the Euler totient function.

1.2 Cyclotomic polynomials and roots of unity

For $n \geq 1$, if ζ is a primitive n–th root of unity, we have, in $\mathbf{C}[t]$,

$$\phi_n(t) = \prod_{\gcd(j,n)=1} (t - \zeta^j).$$

For $n \geq 1$, $\phi_n(t)$ is the irreducible polynomial over $\mathbf{Q}$ of the primitive n–th roots of unity.

Let K be a field and let n be a positive integer. Assume that K has characteristic either 0 or else a prime number p prime to n. Then the polynomial $\phi_n(t)$ is separable over K and its roots in K are exactly the primitive n–th roots of unity which belong to K.

1.3 Properties of $\phi_n(t)$

• For $n \geq 2$ we have

$$\phi_n(t) = t^{\varphi(n)}\phi_n(1/t)$$

• Let $n = p_1^{e_1} \cdots p_r^{e_r}$ where $p_1, \ldots, p_r$ are different primes, $e_0 \geq 0$, $e_i \geq 1$ for $i = 1, \ldots, r$ and $r \geq 1$. Denote by $R = p_1 \cdots p_r$ the radical of n. Then, $\phi_n(t) = \phi_R(t^{n/R})$. For instance $\phi_{2^e}(t) = t^{2^{e-1}} + 1$ for $e \geq 1$.
• Let $n = 2m$ with m odd ≥ 3. Then $\phi_n(t) = \phi_m(-t)$.

$\boxed{\phi_n(1)}$

For $n \geq 2$, we have $\phi_n(1) = e^{\Lambda(n)}$, where the von Mangoldt function Λ is defined for $n \geq 1$ as

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^r \text{ with } p \text{ prime and } r \geq 1; \\ 0 & \text{otherwise.} \end{cases}$$

In other terms, for $n \geq 2$, we have

$$\phi_n(1) = \begin{cases} p & \text{if } n = p^r \text{ with } p \text{ prime and } r \geq 1; \\ 1 & \text{otherwise } (\omega(n) \geq 1). \end{cases}$$

$\boxed{\phi_n(-1)}$

For $n \geq 3$,

$$\phi_n(-1) = \begin{cases} 1 & \text{if } n \text{ is odd;} \\ \phi_{n/2}(1) & \text{if } n \text{ is even.} \end{cases}$$

In other terms, for $n \geq 3$,

$$\phi_n(-1) = \begin{cases} p & \text{if } n = 2p^r \text{ with } p \text{ prime and } r \geq 1; \\ 1 & \text{otherwise.} \end{cases}$$

Hence, $\phi_n(-1) = 1$ when n is odd or when $n = 2m$ where m has at least two distinct prime divisors.

1.4 Lower bound for $\phi_n(t)$

For $n \geq 3$, the polynomial $\phi_n(t)$ is monic, has real coefficients and no real root, hence, it takes only positive values (and its degree $\varphi(n)$ is even).

Lemma 1. *For $n \geq 3$ and $t \in \mathbf{R}$, we have*

$$\phi_n(t) \geq 2^{-\varphi(n)}.$$

Consequence: from $\phi_n(t) = t^{\varphi(n)}\phi_n(1/t)$ we deduce, for $n \geq 3$ and $t \in \mathbf{R}$,

$$\phi_n(t) \geq 2^{-\varphi(n)} \max\{1, |t|\}^{\varphi(n)}. \tag{1.1}$$

Hence, $\phi_n(t) \geq 2^{-\varphi(n)}$ for $n \geq 3$ and $t \in \mathbf{R}$.

Proof of Lemma 1. Let ζ_n be a primitive n-th root of unity in $\mathbf{C}$; then

$$\phi_n(t) = \mathrm{Norm}_{\mathbf{Q}(\zeta_n)/\mathbf{Q}}(t - \zeta_n) = \prod_{\sigma}(t - \sigma(\zeta_n)),$$

where σ runs over the embeddings $\mathbf{Q}(\zeta_n) \to \mathbf{C}$. We have

$$|t - \sigma(\zeta_n)| \geq |\mathrm{Im}(\sigma(\zeta_n))| > 0 \quad \text{and} \quad (2i)\mathrm{Im}(\sigma(\zeta_n)) = \sigma(\zeta_n) - \overline{\sigma(\zeta_n)} = \sigma(\zeta_n - \overline{\zeta_n}).$$

Now $(2i)\mathrm{Im}(\zeta_n) = \zeta_n - \overline{\zeta_n} \in \mathbf{Q}(\zeta_n)$ is an algebraic integer, hence,

$$2^{\varphi(n)}\phi_n(t) \geq |\mathrm{Norm}_{\mathbf{Q}(\zeta_n)/\mathbf{Q}}((2i)\mathrm{Im}(\zeta_n))| \geq 1.$$

□

2 The cyclotomic binary forms

2.1 Definition

For $n \geq 2$, define

$$\Phi_n(X, Y) = Y^{\varphi(n)}\phi_n(X/Y).$$

This is a binary form in $\mathbf{Z}[X, Y]$ of degree $\varphi(n)$. From (1.1) we deduce

Lemma 2 ([G]). *For $n \geq 3$ and $(x, y) \in \mathbf{Z}^2$,*

$$\Phi_n(x, y) \geq 2^{-\varphi(n)} \max\{|x|, |y|\}^{\varphi(n)}.$$

Therefore, if $\Phi_n(x, y) = m$, then

$$\max\{|x|, |y|\} \leq 2m^{1/\varphi(n)}. \tag{2.1}$$

As a consequence, if $\max\{|x|, |y|\} \geq 3$, then n is bounded:

$$\varphi(n) \leq \frac{\log m}{\log(3/2)}.$$

2.2 Generalization to CM fields

The same proof yields:

Proposition 3 ([GL, G]). *Let K be a CM field of degree d over $\mathbf{Q}$. Let $\alpha \in K$ be such that $K = \mathbf{Q}(\alpha)$; let f be the irreducible polynomial of α over $\mathbf{Q}$ and let $F(X, Y) = Y^d f(X/Y)$ the associated homogeneous binary form:*

$$f(t) = a_0 t^d + a_1 t^{d-1} + \cdots + a_d, \qquad F(X, Y) = a_0 X^d + a_1 X^{d-1} Y + \cdots + a_d Y^d.$$

For $(x, y) \in \mathbf{Z}^2$ we have

$$x^d \leq 2^d a_d^{d-1} F(x, y) \quad \text{and} \quad y^d \leq 2^d a_0^{d-1} F(x, y).$$

The estimate of Proposition 3 is best possible: let $n \geq 3$, not of the form p^a nor $2p^a$ with p prime and $a \geq 1$, so that $\phi_n(1) = \phi_n(-1) = 1$. Then the binary form $F_n(X, Y) = \Phi_n(X, Y - X)$ has degree $d = \varphi(n)$ and $a_0 = a_d = 1$. For $x \in \mathbf{Z}$ we have $F_n(x, 2x) = \Phi_n(x, x) = x^d$. Hence, for $y = 2x$, we have

$$y^d = 2^d a_0^{d-1} F(x, y).$$

2.3 Improvement of Győry's estimate for binary cyclotomic forms [FLW]

We improve the upper bound (2.1) in order to have a non trivial result also for $\max\{|x|, |y|\} = 2$.

Theorem 4 ([FLW]). *Let m be a positive integer and let n, x, y be rational integers satisfying $n \geq 3$, $\max\{|x|, |y|\} \geq 2$ and $\Phi_n(x, y) = m$. Then*

$$\max\{|x|, |y|\} \leq \frac{2}{\sqrt{3}}\, m^{1/\varphi(n)}, \quad \textit{hence,} \quad \varphi(n) \leq \frac{2}{\log 3} \log m.$$

These estimates are optimal, since for $\ell \geq 1$, we have $\Phi_3(\ell, -2\ell) = 3\ell^2$. If we assume $\varphi(n) > 2$, which means $\varphi(n) \geq 4$, then

$$\varphi(n) \leq \frac{4}{\log 11} \log m$$

which is best possible since $\Phi_5(1, -2) = 11$.

2.4 Lower bound for the cyclotomic polynomials

Theorem 4 is equivalent to the following result:

Proposition 5 ([FLW]). *For $n \geq 3$ and $t \in \mathbf{R}$,*

$$\phi_n(t) \geq \left(\frac{\sqrt{3}}{2}\right)^{\varphi(n)}.$$

2.5 The sequence $(c_n)_{n\geq 3}$

Define

$$c_n = \inf_{t \in \mathbf{R}} \phi_n(t) \qquad (n \geq 3).$$

Hence, for x and y in $\mathbf{Z}$ and for $n \geq 3$ we have

$$\Phi_n(x, y) \geq c_n \max\{|x|, |y|\}^{\varphi(n)}.$$

According to Proposition 5, for $n \geq 3$ we have

$$c_n \geq \left(\frac{\sqrt{3}}{2}\right)^{\varphi(n)}.$$

Let $n \geq 3$. Write $n = 2^{e_0} p_1^{e_1} \cdots p_r^{e_r}$ where $p_1, \ldots, p_r$ are odd primes with $p_1 < \cdots < p_r$, $e_0 \geq 0$, $e_i \geq 1$ for $i = 1, \ldots, r$ and $r \geq 0$. Then
(i) For $r = 0$, we have $e_0 \geq 2$ and $c_n = c_{2^{e_0}} = 1$.
(ii) For $r \geq 1$ we have

$$c_n = c_{p_1 \cdots p_r} \geq p_1^{-2^{r-2}}.$$

The main step in the proof of Proposition 5 is the following:

Lemma 6 ([FLW]). *For any odd squarefree integer $n = p_1 \cdots p_r$ with $p_1 < p_2 < \cdots < p_r$ satisfying $n \geq 11$ and $n \neq 15$, we have*

$$\varphi(n) > 2^{r+1} \log p_1.$$

Further properties of the sequence $(c_n)_{n\geq 3}$.
- $\liminf_{n\to\infty} c_n = 0$ and $\limsup_{n\to\infty} c_n = 1$.
- The sequence $(c_p)_{p \text{ odd prime}}$ is decreasing from $3/4$ to $1/2$.
- For p_1 and p_2 primes, $c_{p_1 p_2} \geq \dfrac{1}{p_1}$.
- For any prime p_1, $\lim_{p_2\to\infty} c_{p_1 p_2} = \dfrac{1}{p_1}$.

3 The sequence $(a_m)_{m\geq 1}$

For each integer $m \geq 1$, the set

$$\left\{(n, x, y) \in \mathbf{N} \times \mathbf{Z}^2 \;\mid\; n \geq 3,\ \max\{|x|, |y|\} \geq 2,\ \Phi_n(x, y) = m\right\}$$

is finite. Let a_m the number of its elements.

The sequence of integers $m \geq 1$ such that $a_m \geq 1$ starts with the following values of a_m

m	3	4	5	7	8	9	10	11	12	13	16	17
a_m	8	16	8	24	4	16	8	8	12	40	40	16

3.1 Online Encyclopedia of Integer Sequences [OEIS]

`Number of representations of integers by cyclotomic binary forms.`
(OEIS A299214) The sequence $(a_m)_{m\geq 1}$ starts with

0, 0, 8, 16, 8, 0, 24, 4, 16, 8, 8, 12, 40, 0, 0, 40, 16, 4, 24, 8, 24, 0, 0, 0, 24, 8, 12, 24, 8, 0, 32, 8, 0,

8, 0, 16, 32, 0, 24, 8, 8, 0, 32, 0, 8, 0, 0, 12, 40, 12, 0, 32, 8, 0, 8, 0, 32, 8, 0, 0, 48, 0, 24, 40, 16, 0, ...

`Integers represented by cyclotomic binary forms`
(OEIS A296095) $a_m \neq 0$ for $m =$

3, 4, 5, 7, 8, 9, 10, 11, 12, 13, 16, 17, 18, 19, 20, 21, 25, 26, 27, 28, 29, 31, 32, 34, 36, 37, 39, 40,

41, 43, 45, 48, 49, 50, 52, 53, 55, 57, 58, 61, 63, 64, 65, 67, 68, 72, 73, 74, 75, 76, 79, 80, 81, 82, ...

`Integers not represented by cyclotomic binary forms`
(OEIS A293654) $a_m = 0$ for $m =$

1, 2, 6, 14, 15, 22, 23, 24, 30, 33, 35, 38, 42, 44, 46, 47, 51, 54, 56, 59, 60, 62, 66, 69, 70, 71, 77,

78, 83, 86, 87, 88, 92, 94, 95, 96, 99, 102, 105, 107, 110, 114, 115, 118, 119, 120, 123, 126, 131, ...

4 Integers represented by cyclotomic binary forms

For $N \geq 1$, let $\mathcal{A}(N)$ be the number of $m \leq N$ which are represented by cyclotomic binary forms: there exists $n \geq 3$ and $(x, y) \in \mathbb{Z}^2$ with $\max(|x|, |y|) \geq 2$ and $m = \Phi_n(x, y)$. This means

$$\mathcal{A}(N) = \#\{m \in \mathbb{N} \mid m \leq N,\ a_m \neq 0\}.$$

Theorem 7 ([FLW])**.** *We have*

$$\mathcal{A}(N) = \alpha \frac{N}{(\log N)^{\frac{1}{2}}} - \beta \frac{N}{(\log N)^{\frac{3}{4}}} + O\left(\frac{N}{(\log N)^{\frac{3}{2}}}\right) \quad \text{as } N \to \infty.$$

The number of positive integers $\leq N$ represented by Φ_4 (namely the sums of two squares) is

$$\alpha_4 \frac{N}{(\log N)^{\frac{1}{2}}} + O\left(\frac{N}{(\log N)^{\frac{3}{2}}}\right).$$

The number of positive integers $\leq N$ represented by Φ_3 (namely $x^2 + xy + y^2$: Loeschian numbers) is

$$\alpha_3 \frac{N}{(\log N)^{\frac{1}{2}}} + O\left(\frac{N}{(\log N)^{\frac{3}{2}}}\right).$$

The number of positive integers $\leq N$ represented by Φ_4 and by Φ_3 is

$$\beta \frac{N}{(\log N)^{\frac{3}{4}}} + O\left(\frac{N}{(\log N)^{\frac{7}{4}}}\right).$$

Theorem 7 holds with $\alpha = \alpha_3 + \alpha_4$.

The number of positive integers $\leq N$ which are sums of two squares is asymptotically $\alpha_4 N(\log N)^{-1/2}$, where

$$\alpha_4 = \frac{1}{2^{\frac{1}{2}}} \cdot \prod_{p \equiv 3 \bmod 4} \left(1 - \frac{1}{p^2}\right)^{-\frac{1}{2}}.$$

`Decimal expansion of Landau-Ramanujan constant` (OEIS A064533)

$$\alpha_4 = 0.764\,223\,653\,589\,220\ \ldots$$

If a and q are two integers, we denote by $\mathcal{P}_{a,q}$ the set of primes $p \equiv a \bmod q$ and by $N_{a,q}$ any integer ≥ 1 satisfying the condition $p \mid N_{a,q} \Longrightarrow p \equiv a \bmod q$.

An integer $m \geq 1$ is of the form $m = \Phi_4(x, y) = x^2 + y^2$ if and only if there exist integers $a \geq 0$, $N_{3,4}$ and $N_{1,4}$ such that $m = 2^a N_{3,4}^2 N_{1,4}$.

An integer $m \geq 1$ is of the form

$$m = \Phi_3(x, y) = \Phi_6(x, -y) = x^2 + xy + y^2$$

if and only if there exist integers $b \geq 0$, $N_{2,3}$ and $N_{1,3}$ such that $m = 3^b N_{2,3}^2 N_{1,3}$.

The number of positive integers $\le N$ which are represented by the quadratic form $X^2 + XY + Y^2$ is asymptotically $\alpha_3 N(\log N)^{-1/2}$ where

$$\alpha_3 = \frac{1}{2^{\frac{1}{2}} 3^{\frac{1}{4}}} \cdot \prod_{p \equiv 2 \bmod 3} \left(1 - \frac{1}{p^2}\right)^{-\frac{1}{2}}.$$

`Decimal expansion of an analog of the Landau-Ramanujan constant for Loeschian numbers` (OEIS A301429)

$$\alpha_3 = \frac{1}{2^{\frac{1}{2}} 3^{\frac{1}{4}}} \cdot \prod_{p \equiv 2 \bmod 3} \left(1 - \frac{1}{p^2}\right)^{-\frac{1}{2}} = 0.638\,909\,405\,44\ \ldots$$

Hence,

$$\alpha = \alpha_3 + \alpha_4 = 1.403\,133\,059\,034\ \ldots$$

Using the method of Flajolet and Vardi, Bill Allombert (private communication, April 2018) computed

$$\begin{aligned}\alpha_3 = {} & 0.63890940544534388225494267492824509375497550802912 \\ & 33454216923657080763100276496582468971791125286643881 4\ldots\end{aligned}$$

`Decimal expansion of an analog of the Landau-Ramanujan constant for Loeschian numbers which are sums of two squares` (OEIS A301430)

$$\begin{aligned}\beta = {} & \frac{3^{\frac{1}{4}}}{2^{\frac{5}{4}}} \cdot \pi^{\frac{1}{2}} \cdot (\log(2+\sqrt{3}))^{\frac{1}{4}} \cdot \frac{1}{\Gamma(1/4)} \cdot \prod_{p \equiv 5,\,7,\,11 \bmod 12} \left(1 - \frac{1}{p^2}\right)^{-\frac{1}{2}} \\ = {} & 0.302\,316\,142\,35\ldots\end{aligned}$$

Using the method of Flajolet and Vardi, Bill Allombert (private communication, April 2018) computed

$$\begin{aligned}\beta = {} & 0.30231614235706563794776990048019971560241279518936964545 88 \\ & 67841288865448752410510899487467813979272708567765913272591 0\ldots\end{aligned}$$

Further developments

• Prove similar estimates for the number of integers represented by other binary forms (done for quadratic forms); e.g.: prove similar estimates for the number of integers which are sums of two cubes, two biquadrates,. . .
• Prove similar estimates for the number of integers which are represented by Φ_n for a given n.
• Prove similar estimates for the number of integers which are represented by Φ_n for some n with $\varphi(n) \geq d$.

5 Representation of integers by positive definite quadratic forms

Theorem 8 (P. Bernays [B]). *Let $F \in \mathbf{Z}[X, Y]$ be a positive definite quadratic form. There exists a positive constant $\mathbf{C}_F$ such that, for $N \to \infty$, the number of positive integers $m \in \mathbf{Z}$, $m \leq N$ which are represented by F is asymptotically $\mathbf{C}_F N(\log N)^{-\frac{1}{2}}$.*

Theorem 9 (Stewart - Xiao [S–Y]). *Let F be a binary form of degree $d \geq 3$ with nonzero discriminant.*

There exists a positive constant $C_F > 0$ such that the number of integers of absolute value at most N which are represented by $F(X, Y)$ is asymptotic to $C_F N^{2/d}$.

Proposition 10 (K. Mahler [M]). *Let F be a binary form of degree $d \geq 3$ with nonzero discriminant. Denote by A_F the area (Lebesgue measure) of the domain*

$$\{(x, y) \in \mathbf{R}^2 \mid F(x, y) \leq 1\}.$$

For $Z > 0$ denote by $N_F(Z)$ the number of $(x, y) \in \mathbf{Z}^2$ such that $0 < |F(x, y)| \leq Z$. Then

$$N_F(Z) = A_F Z^{2/d} + O(Z^{1/(d-1)})$$

as $Z \to \infty$.

The situation for positive definite forms of degree ≥ 3 is different for the following reason: if a positive integer m is represented by a positive definite quadratic form, it usually has many such representations; while if a positive integer m is represented by a positive definite binary form of degree $d \geq 3$, it usually has few such representations. If F is a positive definite quadratic form, the number of (x, y) with $F(x, y) \leq N$ is asymptotically a constant times N, but the number of $F(x, y)$ is much smaller.

If F is a positive definite binary form of degree $d \geq 3$, the number of (x, y) with $F(x, y) \leq N$ is asymptotically a constant times $N^{1/d}$, the number of $F(x, y)$ is also asymptotically a constant times $N^{1/d}$.

Sums of k–th powers

If a positive integer m is a sum of two squares, there are many such representations. Indeed, the number of (x, y) in $\mathbf{Z} \times \mathbf{Z}$ with $x^2 + y^2 \leq N$ is asymptotic to πN, while the number of values $\leq N$ taken by the quadratic form Φ_4 is asymptotic to $\alpha_4 N/\sqrt{\log N}$ where α_4 is the Landau–Ramanujan constant. Hence, Φ_4 takes each of these values with a high multiplicity, on the average $(\pi/\alpha)\sqrt{\log N}$.

On the opposite, it is extremely rare that a positive integer is a sum of two biquadrates in more than one way (not counting symmetries).

$635\,318\,657 = 158^4 + 59^4 = 134^4 + 133^4$. Leonhard Euler1707 – 1783

The smallest integer represented by x^4+y^4 in two essentially different ways was found by Euler, it is $635318657 = 41 \cdot 113 \cdot 241 \cdot 569$.

`Number of solutions to the equation` $x^4 + y^4 = n$ `with` $x \geq y > 0$ (OEIS A216284)

An infinite family with one parameter is known for non trivial solutions to $x_1^4 + x_2^4 = x_3^4 + x_4^4$, see:

`http://mathworld.wolfram.com/DiophantineEquation4thPowers.html`

Sums of k–th powers

One conjectures that given $k \geq 5$, if an integer is of the form $x^k + y^k$, there is essentially a unique such representation. But there is no value of k for which this has been proved.

The situation for positive definite forms of degree ≥ 3 is different also for the following reason. A necessary and sufficient condition for a number m to be represented by one of the quadratic forms Φ_3, Φ_4, is given by a congruence. By contrast, consider the quartic binary form $\Phi_8(X, Y) = X^4 + Y^4$. On the one hand, an integer represented by Φ_8 is of the form

$$N_{1,8}(N_{3,8}N_{5,8}N_{7,8})^4.$$

On the other hand, there are many integers of this form which are not represented by Φ_8.

`Quartan primes: primes of the form` x^4+y^4, $x > 0$, $y > 0$ (OEIS A002645)

The list of prime numbers represented by Φ_8 start with

2, 17, 97, 257, 337, 641, 881, 1297, 2417, 2657, 3697, 4177, 4721, 6577, 10657, 12401, 14657, 14897, 15937, 16561, 28817, 38561, 39041, 49297, 54721, 65537, 65617, 66161, 66977, 80177, ...

It is not known whether this list is finite or not.

The largest known quartan prime is currently the largest known generalized Fermat prime: The 1353265-digit $(145310^{65536})^4 + 1^4$.

Primes of the form $x^{2^k} + y^{2^k}$ (See https://oeis.org/)

[OEIS A002313] `primes of the form` $x^2 + y^2$.

[OEIS A002645] `primes of the form` $x^4 + y^4$,

[OEIS A006686] `primes of the form` $x^8 + y^8$,

[OEIS A100266] `primes of the form` $x^{16} + y^{16}$,

[OEIS A100267] `primes of the form` $x^{32} + y^{32}$.

But it is known that there are infinitely many prime numbers of the form $X^2 + Y^4$ [FI].

References

[B] P. Bernays *Über die Darstellung von positiven, ganzen Zahlen durch die primitiven, binären quadratischen Formen einer nicht quadratischen Diskriminante*, Ph.D. dissertation, Georg-August-Universität, Göttingrn, Germany, 1912.

[FLW] Č.E. Fouvry, C. Levesque & M. Waldschmidt. *R*epresentation of integers by cyclotomic binary forms. *Acta Arithmetica*, **184** 1 (2018), 67 – 86.

[FI] J. Friedlander & H. Iwaniec *The polynomial $X^2 + Y^4$ captures its primes*. *Ann. of Math.* (2) **148** (1998), no. 3, 945 –1040.

[G] K. Győry *Représentation des nombres entiers par des formes binaires*, *Publ. Math. Debrecen* **2**4 (3–4), 363 – 375, (1977).

[GL] K. Győry & L. Lovász *Representation of integers by norm forms II*, *Publ. Math. Debrecen* **17**, 173 – 181, (1970).

[M] K. Mahler *Ęber die mittlere Anzahl der Darstellungen grosser Zahlen durch binŁre Formen. Acta Math.* **62** (1933), 91–166.

[OEIS] N.J. Sloane *The On–line Encyclopedia of Integer Sequences*, (`https://oeis.org/`)

[S–Y] C.L. Stewart & S. Yao Xiao *On the representation of integers by binary forms*,

Part 2

Contributed Talks

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 4, *Number* 1, *March* 2019, *pages* 117-118

Unlikely Intersections in families of abelian varieties

Fabrizio Barroero

Let n be an integer with $n \geq 2$ and let E_λ denote the elliptic curve in the Legendre form defined by $Y^2 = X(X-1)(X-\lambda)$. Masser and Zannier showed that there are at most finitely many complex numbers $\lambda_0 \neq 0, 1$ such that the two points $\left(2, \sqrt{2(2-\lambda_0)}\right)$ and $\left(3, \sqrt{6(3-\lambda_0)}\right)$ both have finite order on the elliptic curve E_{λ_0}. Later Masser and Zannier proved that one can replace 2 and 3 with any two distinct complex numbers ($\neq 0, 1$) or even choose distinct X-coordinates ($\neq \lambda$) defined over an algebraic closure of $\mathbb{C}(\lambda)$.

In his book, Zannier asks if there are finitely many $\lambda_0 \in \mathbb{C}$ such that two independent relations between the points $\left(2, \sqrt{2(2-\lambda_0)}\right)$, $\left(3, \sqrt{6(3-\lambda_0)}\right)$ and $\left(5, \sqrt{20(5-\lambda_0)}\right)$ hold on E_{λ_0}.

In joint work with Laura Capuano we proved that this question has a positive answer, as Zannier expected in view of very general conjectures. We actually showed a more general result, analogous to the one of Masser and Zannier.

Theorem 1 *Let $C \subseteq \mathbb{A}^{2n+1}$ be an irreducible curve defined over $\overline{\mathbb{Q}}$ with coordinate functions $(x_1, y_1, \ldots, x_n, y_n, \lambda)$, λ non-constant, such that, for every $j = 1, \ldots, n$, the points $P_j = (x_j, y_j)$ lie on E_λ and there are no integers $a_1, \ldots, a_n \in \mathbb{Z}$, not all zero, such that $a_1 P_1 + \cdots + a_n P_n = O$*

identically on C. Then there are at most finitely many $\mathbf{c} \in C$ such that the points $P_1(\mathbf{c}), \ldots, P_n(\mathbf{c})$ satisfy two independent relations on $E_{\lambda(\mathbf{c})}$.

In later works we extended the theorem to abelian schemes.

Fix a number field k and a smooth irreducible curve S defined over k. We consider an abelian scheme $\mathcal{A}$ over S of relative dimension $g \geq 2$, also defined over k. This means that for each $s \in S(\mathbb{C})$ we have an abelian variety $\mathcal{A}_s$ of dimension g defined over $k(s)$.

Let C be an irreducible curve in $\mathcal{A}$ also defined over k and not contained in a proper subgroup scheme of $\mathcal{A}$, even after a base extension. A component of a subgroup scheme of $\mathcal{A}$ is either a component of an algebraic subgroup of a fiber or it dominates the base curve S. A subgroup scheme whose irreducible components are all of the latter kind is called flat.

The following theorem follows from joint works with Laura Capuano and a work of Habegger and Pila in the iso-trivial case.

Theorem 2 *Let k and S be as above. Let $\mathcal{A} \to S$ be an abelian scheme and C an irreducible curve in $\mathcal{A}$ not contained in a proper subgroup scheme of $\mathcal{A}$, even after a finite base change. Suppose that $\mathcal{A}$ and C are defined over k. Then, the intersection of C with the union of all flat subgroup schemes of $\mathcal{A}$ of codimension at least 2 is a finite set.*

Fabrizio Barroero
Departement Mathematik und Informatik
Universität Basel
Spiegelgasse 1
4051 Basel, Switzerland.
email: fbarroero@gmail.com

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 4, *Number* 1, *March* 2019, *pages* 119-120

The Sierpiński d-dimensional tetrahedron and a Diophantine nonlinear system

Fabio Caldarola

The Sierpiński tetrahedron Δ^d is the d-dimensional generalization of the most known Sierpiński gasket which appears in many fields of mathematics and applied sciences. Starting from a generating sequence of d-polytopes $\left\{\Delta_n^d\right\}_n$ for Δ^d $\left(\text{where } \Delta_0^d \text{ is the unitary } d\text{-simplex}\right)$, we find closed formulas for the sum $v_n^{d,\,k}$ of the measures of the k-dimensional elements of Δ_n^d, deducing the behavior of the sequences $\left\{v_n^{d,\,k}\right\}_n$ at infinity, both in traditional analysis and in a recently proposed setting based on the symbol ①. The interesting point for us is that the use of such a new framework (just at a notational level) lead us to formulate several problems in form of Diophantine systems, which can be studied and investigated in terms of classical number theory by working with traditional tools from algebra, analysis, etc.
Complex problems arise in this way and, in particular, in the considered case we come to the following Diophantine system (see [1] for details)

$$\begin{cases} \dfrac{\sqrt{k+1}}{k!\sqrt{2^k}} \cdot \dbinom{d+1}{k+1} = \dfrac{\sqrt{h+1}}{h!\sqrt{2^h}} \cdot \dbinom{t+1}{h+1} \\ \dfrac{d+1}{2^k} = \dfrac{t+1}{2^h} \end{cases} . \tag{1}$$

Equations like the previous are not properly "Diophantine" because this word usually refers only to equations of polynomial or exponential type. Moreover, they are not very present in literature and still very little studied: just few authors call them *binomial Diophantine equations*.

The problem of deciding whether there are nontrivial integer solutions of a system like (1), and if so to find them all, is not a simple matter in general; for example, by using the most powerful scientific computational software available today (like, for instance, *Mathematica*® 11.0 or many others) it is not possible to obtain any answer except for very small values of d and t, cause the complexity of (1).

In conclusion, while if we vary the size of the starting d-simplex Δ_0^d in an appropriate way we achieve systems with nontrivial integer solutions, in our case instead, as consequence of stronger theoretical results, we obtain the following

Corollary 1 *There are no integer solutions* $(d,t,k,h) \in \mathbb{N}^4$ *of the system* (1)*, such that* $1 \leqslant k \leqslant d$*,* $1 \leqslant h \leqslant t$ *and* $2 \leqslant d < t$.

References

[1] Caldarola F. The exact measures of the Sierpinski d-dimensional tetrahedron in connection with a Diophantine nonlinear system, Comm Nonlinear Sci Num Simul 63 (2018), 228–238.

[2] Caldarola F. The Sierpinski curve viewed by numerical computations with infinities and infinitesimals, Appl. Math. Comput. 318 (2018), 321–328.

Fabio Caldarola
Dep. of Mathematics and Computer Science
University of Calabria
Cubo 31/B, Ponte P. Bucci
87036 Arcavacata di Rende (CS), ITALY .
email: caldarola@mat.unical.it

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 4, *Number* 1, *March* 2019, *pages* 121-122

Explicit formula for the average of Goldbach and prime tuples representations

Marco Cantarini

We prove an explicit formula and an asymptotic formula for the average of the functions $r_G(n) = \sum_{\substack{m_1,m_2\leq n\\ m_1+m_2=n}} \Lambda(m_1)\Lambda(m_2)$ and $r_{PT}(N,h) = \sum_{n=0}^{N} \Lambda(n)\Lambda(n+h)$, $h \in \mathbb{N}$, which are the counting function of the Goldbach numbers and the counting function of the prime tuples, respectively. We will find an explicit formula and we will prove that it is possible write it as an asymptotic formula with three terms and an error term $O(N)$ without the assumption of the Riemann hypothesis (RH for brevity). We prove the following

Theorem 1 *Let $N > 2$ be an integer. Then*

$$\sum_{n\leq 2N} r_G(n) - \frac{r_G(2N)}{2} = 2N^2 - 2\sum_{\rho} \frac{(2N-2)^{\rho+1}}{\rho(\rho+1)} +$$

$$+2\sum_{\rho_1} (2N)^{\rho_1} \left(\Gamma(\rho_1) \sum_{\rho_2} \frac{(2N)^{\rho_2}\Gamma(\rho_2)}{\Gamma(\rho_1+\rho_2+1)} - \sum_{\rho_2} \frac{(2N)^{\rho_2}}{\rho_2} \cdot \mathcal{B} \right) + F(N)$$

where

$$\mathcal{B} = \left(B_{1/N}(\rho_2+1,\rho_1) + B_{1/2}(\rho_1,\rho_2+1) \right),$$

$B_z(a,b)$ is the incomplete Beta function, $\rho = \beta + i\gamma$ (with or without subscript) runs over the non-trivial zeros of the Riemann Zeta function $\zeta(s)$, and $F(N)$ is a function that can be explicitly calculated in terms of elementary functions, series over non-trivial zeros, Dilogarithm and incomplete Beta functions, satisfying $F(N) = O(N)$, as N goes to infinity.

We are also able to find a truncated version of this formula (like the classical explicit formula of $\psi(x) = \sum_{n \leq x} \Lambda(n)$.). It is interesting to note that if we assume the third term of the explicit formula in Theorem 1 grows in a suitable way as $N \to \infty$ then we can prove that every interval $[2N, 2N + 2H]$, where $H = H(N)$ is an appropriate function of N, contains a Goldbach number. Using the same ideas of Theorem 1 we also find a completely explicit formula for $r_{PT}(N, h)$.

Marco Cantarini
Dipartimento di Scienze Matematiche, Fisiche e Informatiche
Università degli Studi di Parma
Parco Area delle Scienze, 53/a
43124 Parma, Italy.

email: cantarini_m@libero.it

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 4, *Number* 1, *March* 2019, *pages* 123-124

New instances of the Mumford–Tate conjecture

Victoria Cantoral-Farfán

Let A be a simple abelian variety defined over a number field K of dimension g. Let $MT(A)$ be the Mumford–Tate group of A, which is an algebraic reductive group defined over $\mathbb{Q}$. Let G_K be the absolute Galois group of K, ℓ a prime number and $T_\ell(A)$ the ℓ-adic Tate module of A. Let us consider the following ℓ-adic representation:

$$\rho_\ell : G_K \to Aut(T_\ell) \simeq GL_{2g}(\mathbb{Z}_\ell).$$

We define the ℓ-adic monodromy group G_ℓ as the Zariski closure of the image of ρ_ℓ, it is an algebraic group over $\mathbb{Q}_\ell$.

Conjecture 0.1 (Mumford–Tate '66) *For every prime number ℓ we have*

$$G_\ell^\circ \simeq MT(A) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell.$$

Definition 0.2 *An abelian variety A is fully of Lefschetz type if A satisfies conjecture 0.1 and $MT(A)$ is the Lefschetz group,* i.e *the group of symplectic similitudes which commutes with endomorphisms.*

An abelian variety is of type III, in the sense of Albert classification, if $D := End_K(A) \otimes \mathbb{Q}$ is an indefinite quaternion algebra over a totally real field $F := Z(D)$ of degree e over $\mathbb{Q}$. Let us denote $h := \frac{g}{2e}$ the relative dimension of A in the type III case.

Theorem 0.3 (C.-F., 2017) *Let A be a simple abelian variety of type III. Assume that one of the two conditions is satisfied:*

1. $h \in \{2k+1,\ k \in \mathbb{N}\} \setminus \left\{\frac{1}{2}\binom{2^{m+2}}{2^{m+1}},\ m \in \mathbb{N}\right\}$;
2. $Z(D) = \mathbb{Q}$ *and* $h \notin \Sigma$

The A is fully of Lefschetz type.

The reader can find the definition of Σ in [Can17], for instance:

$$\Sigma = \{4, 6, 8, 16, 36, 64, 70, 100, 128, 144, 196, 216, 256, 324, 400, 484\}.$$

Further applications of this theorem 0.3 can be found in the direction of the Algebraic Sato–Tate conjecture stated by Banaszak and Kedlaya in [BK15]. For instance we can give a new list of abelian varieties which are fully of Lefschetz type and such that the twisted Lefschetz group is connected. In that scenario, those abelian varieties satisfy the Algebraic Sato–Tate conjecture.

References

[BK15] G. Banaszak and K. Kedlaya, *An algebraic Sato-Tate group and Sato-Tate conjecture*, Indiana Univ. Math. J. **64** (2015), no. 1, 245 –274. ↑124

[Can17] V. Cantoral-Farfán, *Torsion for abelian varieties of type III*, ArXiv e-prints (2017), available at 1711.04813. ↑124

Victoria Cantoral-Farfán
Math section
ICTP
11 strada Costiera
34151, Trieste, Italy.
email: vcantora@ictp.it

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 4, *Number* 1, *March* 2019, *pages* 125-126

Expansions of quadratic numbers in a p-adic continued fraction

Laura Capuano

The theory of real continued fractions plays a central role in real Diophantine Approximation for many different reasons, in particular because the convergents of the simple continued fraction expansion of a real number α give the best rational approximations to α. Motivated by the same type of questions, several authors (Mahler, Schneider, Ruban, Bundschuch and Browkin) have generalized the theory of real continued fractions to the ℓ-adic case in various ways.

The theory of ℓ-adic continued fractions presents many differences with respect to the real case. First of all, there is no canonical way to define a continued fraction expansion in this context, as the expansion depends on the chosen system of residues mod ℓ, and the basic properties of finiteness and periodicity change with this choice. The ℓ-adic process which is the most similar to the classical real one was mentioned for the first time in one of the earliest papers on the subject by Mahler and then studied accurately by Ruban, who showed that these continued fractions enjoy nice ergodic properties.

In a joint work with F. Veneziano and U. Zannier we investigate questions about finiteness and periodicity of Ruban's continued fraction expansions.

In the classical real case, a real number has finite continued fraction expansion if and only if the number is rational, and Lagrange's theorem

ensures that a real number has an infinite periodic continued fraction expansion if and only if it is quadratic irrational.

For Ruban's continued fraction expansion instead, also rational numbers can have periodic continued fractions, as showed by Laohakosol and independently by Wang. Moreover, for quadratic irrationals, no full analogue of Lagrange's theorem holds, as showed by Ooto, but it was not known how to decide whether the expansion for a given quadratic number is or is not periodic. In our work, we give a completely general algorithm in this sense which, somewhat surprisingly, depends on the "real" values of the complete quotients appearing in the ℓ-adic continued fraction expansion:

Theorem 1 *Let $\alpha \in \mathbb{Q}_\ell \setminus \mathbb{Q}$ be a quadratic irrational over $\mathbb{Q}$. Then, the Ruban continued fraction expansion of α is periodic if and only if there exists a unique real embedding $j : \mathbb{Q}(\alpha) \to \mathbb{R}$ such that the image of each complete quotient α_n under the map j is positive.*

Moreover, there is an effective constant N_α with the property that, either $\exists\, n \leq N_\alpha$ such that α_n does not have a positive real embedding, and therefore the expansion is not periodic, or $\exists\, n_1 < n_2 \leq N_\alpha$ such that $\alpha_{n_1} = \alpha_{n_2}$, hence the expansion is periodic.

If $\alpha \in \mathbb{Q}_\ell$ is of the form $\alpha = \frac{b+\sqrt{\Delta}}{c}$ with b, c, Δ integers and $\Delta > 0$ not a square in $\mathbb{Q}_\ell$, then the constant N_α in the Theorem can be taken equal to $bc + 2(c\sqrt{\Delta} + 1)^3$.

Capuano Laura
Mathematical Institute
University of Oxford
Andrew Wiles Building
Woodstock Road
OX2 6GG Oxford UK.
email: Laura.Capuano@maths.ox.ac.uk

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 4, *Number* 1, *March* 2019, *pages* 127-128

Correlations of Ramanujan expansions

Giovanni Coppola

The *c*orrelation ("*s*hifted convolution sum") of any $f, g : \mathbf{N} \to \mathbf{C}$ is

$$C_{f,g}(N,a) \stackrel{def}{=} \sum_{n \le N} f(n)g(n+a). \tag{1}$$

The integer $a > 0$ is the *s*hift. Classic heuristic:

$$C_{f,g}(N,a) \sim S_{f,g}(a)N, \quad S_{f,g}(a) \stackrel{def}{=} \sum_{q=1}^{\infty} \widehat{f}(q)\widehat{g}(q)c_q(a), \tag{2}$$

$S_{f,g}$ is the *s*ingular series and $c_q(a) \stackrel{def}{=} \sum_{j \in \mathbf{Z}_q^*} \cos(2\pi ja/q)$ is the *Ramanujan sum*. Now $S_{f,g}$ is a finite sum, from **Vital Remark:** we have **finite Ramanujan coefficients** $\hat{f}, \hat{g}$, by $f' \stackrel{def}{=} f * \mu$, $g' \stackrel{def}{=} g * \mu$ and Möbius inversion

$$\widehat{f}(q) \stackrel{def}{=} \sum_{\substack{d \le N \\ d \equiv 0 \bmod q}} \frac{f'(d)}{d}, \ \widehat{g}(q) \stackrel{def}{=} \sum_{\substack{d \le N+a \\ d \equiv 0 \bmod q}} \frac{g'(d)}{d}. \tag{3}$$

With Ram Murty we found the **R**amanujan **e**xact **e**xplicit **f**ormula [J.Number Theory 185(2018),16–47] (here $\varphi(q)$ is *E*uler function):

$$C_{f,g}(N,a) = \sum_{q \le N} \frac{\widehat{g}(q)}{\varphi(q)} \sum_{n \le N} f(n)c_q(n)c_q(a). \tag{Reef}$$

It is **n**ot for free: under **B**asic **H**ypotheses, needs some conditions. On [JNT,Th.1] we gave 3 equivalent ones. We give now other 4.

As usual $\omega(d) \stackrel{def}{=} |\{p \text{ prime} : p \text{ divides } d\}|$ and the *Eratosthenes Transform* (**E.t.** for short) of $C_{f,g}$ is

$$C'_{f,g}(N,d) \stackrel{def}{=} \sum_{t|d} C_{f,g}(N,t)\mu(d/t).$$

Under **BH** (Th.1 hypotheses), Reef's equivalent to (F.A.E.):

$$(Delange\ \ Hypothesis) \qquad \sum_{d} 2^{\omega(d)} \left| C'_{f,g}(N,d) \right| / d < \infty$$

$$(E.t.Reef) \qquad C'_{f,g}(N,d) = d \sum_{k \le \frac{Q}{d}} \frac{\mu(k)\widehat{g}(dk)}{\varphi(dk)} \sum_{n \le N} f(n) c_{dk}(n)$$

$$\sum_{d>Q} \frac{1}{d} C'_{f,g}(N,d) \sum_{\substack{\ell > Q \\ \ell | d}} c_\ell(a) = 0, \quad \forall a \in \mathbf{N}$$

$$\lim_{T \to \infty} \sum_{\ell \le T} \sum_{\substack{d > T \\ d \equiv 0 \bmod \ell}} \frac{1}{d} C'_{f,g}(N,d) c_\ell(a) = 0, \quad \forall a \in \mathbf{N}$$

Giovanni Coppola
University of Salerno
Home:Via Partenio
83100 Avellino ITALY.
email: giovanni.coppola@unina.it

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 4, *Number* 1, *March* 2019, *pages* 129-130

Correlations of Multiplicative Functions

Pranendu Darbar

Let $g_j : \mathbb{N} \to \mathbb{C}$ be multiplicative functions such that $|g_j(n)| \leq 1$ for all n. Let $F_1(x), F_2(x), F_3(x)$ are relatively co-prime polynomials.

Consider the following triple correlation function:

$$M_x(g_1, g_2, g_3) = \frac{1}{x} \sum_{n \leq x} g_1(F_1(n)) g_2(F_2(n)) g_3(F_3(n)). \tag{1}$$

In [KAT], Kátai studied the asymptotic bahaviour of the above sum (1) when $F_j(x)$ are special polynomials but did not provide error term. In [ST4], Stepanauskas studied the asymptotic formula for sum (1) with explicit error term when $F_j(x), j = 1, 2, 3$ are linear polynomials.

The aim of the article [DAR] is to prove the following statement:

Theorem 1 *Let $F_j(x), j = 1, 2, 3$ be polynomials as above of degree greater than or equal to 2. Let g_1, g_2 and g_3 be multiplicative functions as above. Then there exists a positive absolute constant c and a natural number γ such that for all $x \geq r \geq \gamma$ and for all $1 - \frac{1}{v_1+v_2+v_3} < \alpha < 1$, we have*

$$M_x(g_1, g_2, g_3) - P'(x) \ll \frac{1}{x} (F_1(x)F_2(x)F_3(x))^{1-\alpha} \exp\left(\frac{cr^\alpha}{\log r}\right)$$
$$+ (T(x))^{\frac{1}{2}} + (S(r, x))^{\frac{1}{2}} + (r \log r)^{-\frac{1}{2}} + \frac{1}{x} C(r, x) + \frac{1}{\log x}$$

where v_j denote the degree of the polynomials $F_j(n)$ respectively.

The following corollary is a direct application of the Theorem 1.

Corollary 2 *Let $\phi(n)$ be Euler's totient function and $\sigma(n) = \sum_{d|n} d$. Let $F_1(x) = x^2 + b, F_2(x) = x^2 + c, F_3(x) = x^2 + d, 0 < t < 1$, where b, c, d are taken such that $F_j(x), j = 1, 2, 3$ satisfies the assumption of Theorem 1 and is a quadratic residue for all odd prime p. Then there exist a natural number γ such that for all $x \geq \gamma$,*

$$\frac{1}{x}\sum_{n\leq x}\frac{\phi(n^2+b)\phi(n^2+c)\phi(n^2+d)}{\sigma(n^2+b)\sigma(n^2+c)\sigma(n^2+d)} = P_1'(\gamma)\prod_{p>\gamma} w_p' + O\left(\frac{1}{(\log x)^t}\right)$$

where $w_p' = \left(1 - \frac{6}{p} + 6\left(1 - \frac{1}{p}\right)^2 \sum_{m=1}^{\infty} \frac{1}{1+p+\cdots+p^m}\right)$.

For more details see [DAR].

References

[DAR] P. Darbar *Triple correlations of multiplicative functions*, Acta Arithmetica, **180**, 2017, pp. 63-88.

[KAT] I. Kátai *On the distribution of Arithmetical functions*, Acta Mathematica Academiae Scientiarum Hungaricae, **20** (1-2), 1969, pp. 60-87.

[ST4] G.Stepanauskas *Mean values of Multiplcative Functions III*, New trends in probability and statistics, **4**, pp. 371âĂŞ387, VSP, Utrecht, 1997

Pranendu Darbar
Mathematics Department
The Institute of Mathematicle Sciences
IV Cross Road, CIT Campus Taramani
Chennai 600 113 Tamil Nadu, India..
email: dpranendu@imsc.res.in

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 4, *Number* 1, *March* 2019, *pages* 131-132

Diophantine approximation problem with 3 prime variables

Alessandro Gambini

We will prove that the inequality

$$|\lambda_1 p_1 + \lambda_2 p_2 + \lambda_3 p_3^k - \omega| \leq (\max(p_1, p_2, p_3^k))^{\psi(k)+\varepsilon}$$

where

$$\psi(k) = \begin{cases} (3-2k)/(6k) & \text{se } 1 < k \leq 6/5 \\ 1/12 & \text{se } 6/5 < k \leq 2 \\ (3-k)/(6k) & \text{se } 2 < k < 3 \\ 1/24 & \text{se } k = 3 \end{cases}$$

has infinitely many solutions in prime variables p_1, p_2 and p_3 for any given real number ω, with λ_1, λ_2 and λ_3 non-zero real numbers, not all of the same sign and such that λ_1/λ_2 is not rational, and $1 < k \leq 3$ real (see [1]).

It is easy to see that the hypothesis on the sign is natural, if one wants to approximate all real numbers, and the hypothesis on the ratio λ_1/λ_2 is necessary to avoid trivial cases where the inequality can not hold.

The values for ψ depend on suitable bounds for the relevant exponential sums over prime powers. The proof uses a variant of the circle method technique introduced by Davenport & Heilbronn where the integration on a circle is replaced by the integration on the whole real line, split in a major arc (that provides the main term), an intermediate

arc, a minor arc and a trivial arc. The contributions of the last three subsets turn out to be small.

In this kind of problems we can not count "exact hits" hence, we need a measure of "proximity" which can be provided in a number of ways, even tough, the crucial property is the rate of vanishing at infinity that must not be too slow.

Theorem is proved on a suitable sequence X_n with limit $+\infty$, related to the convergent of the fraction λ_1/λ_2 exploiting the fact that we know that there exist infinitely many solutions of the inequality

$$\left|\frac{\lambda_1}{\lambda_2} - \frac{a}{q}\right| < \frac{1}{q^2}.$$

The main tools used to proved the Theorem are suitable estimations of the L^n-norm of the exponential sums over primes and the Harman technique on the minor arc.

References

[1] A. Gambini, A. Languasco, and A. Zaccagnini. A Diophantine approximation problem with two primes and one k-th power of a prime. *Journal of Number Theory*, 188:210—228, 2018.

Alessandro Gambini
Dipartimento di Scienze, Matematiche, Fisiche e Informatiche
Universitá di Parma
Parco Area delle Scienze 53/a
43124 Parma, Italy.
email: a.gambini@unibo.it

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 4, *Number* 1, *March* 2019, *pages* 133-134

Counting rational points on genus one curves

Manh Hung Tran

We study the density of rational points on genus one curves C by giving uniform upper bounds for the counting function

$$N(C, B) := \sharp\{P \in C(\mathbb{Q}) : H(P) \leq B\},$$

where the height function H is defined as $H(P) := \max\{|x_0|, ..., |x_n|\}$ for $P = [x_0, ..., x_n]$ with $\gcd(x_0, ..., x_n) = 1$. The main tools to study this problem are descent and determinant methods. We proved new results for genus one curves in two important forms: smooth plane cubic curves and complete intersections of two quadrics in $\mathbb{P}^3$.

Let $C \subset \mathbb{P}^2$ be a smooth cubic curve and r=rank(Jac(C)), then for any positive integer m

$$N(C, B) \ll m^r \left(B^{\frac{2}{3m^2}} + m^2\right) \log B.$$

Taking $m = 1 + [\sqrt{\log B}]$ we obtain $N(C, B) \ll (\log B)^{2+r/2}$. This should be compared with the classical non-uniform bound of Néron: $N(C, B) \sim c_F(\log B)^{r/2}$.

For a non-singular quartic curve C in $\mathbb{P}^3$ defined by a complete intersection of two quadric surfaces $Q_1 = 0$ and $Q_2 = 0$, where $Q_1, Q_2 \in \mathbb{Z}[x_0, x_1, x_2, x_3]^{(2)}$. Then C is also of genus one and Jac(C) is an elliptic

curve and again we can use descent argument. We obtain similar estimates as in cubic case

$$N(C,B) \ll m^r \left(B^{\frac{1}{2m^2}} + \log B\right) \log B$$

and

$$N(C,B) \ll (\log B)^{2+r/2}.$$

Moreover, we obtain completely uniform bound for genus one curves in $\mathbb{P}^3$ given in diagonal forms:

$$C : \begin{cases} a_0x_0^2 + a_1x_1^2 + a_2x_2^2 + a_3x_3^2 = 0 \\ b_0x_0^2 + b_1x_1^2 + b_2x_2^2 + b_3x_3^2 = 0 \end{cases}$$

This class contains examples of elliptic curves with arbitrary j-invariants. The main result is

$$N(C,B) \ll_\varepsilon B^{1/2-3/392+\varepsilon}.$$

Manh Hung Tran
Department of Mathematical Sciences
Chalmers University of Technology
Chalmers Tvargata 3
41296 Gothenburg, Sweden.
email: manhh@chalmers.se

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 4, *Number* 1, *March* 2019, *pages* 135-136

On the Báez-Duarte criterion for the Riemann hypothesis

Goubi Mouloud

This work is an attempt to prove the existence of a Family of Beurling functions satisfying Báez-Duarte Criterion for Riemann Hypothesis.

Let the Hilbert space $\mathcal{H} = L^2\left([0,+\infty[, t^{-2}dt\right)$ with the inner product $\langle f, g\rangle = \int_0^{+\infty} f(t)\overline{g(t)}t^{-2}dt$. For any integer n let as consider the functions e_n defined over $\mathcal{H}$ by $e_n(t) = \left\{\frac{t}{n}\right\}$. Only the Beurling functions are of the form $f_n = ce_1 + g_n$ where g_n is the sum $\sum_{k=2}^{n} c_k v_k$ and $v_k(t) = e_n(\lfloor t\rfloor)$.
Supposing that $\sum_{k\geq 0}\frac{g_n(k)}{k(k+1)}$, $\langle e_1, g_n\rangle$ and $\sum_{k\geq 0}\frac{g_n^2(k)}{k(k+1)}$ are converging respectively to α, λ and β when n tends to infinity. And using technics from Hilbert geometry, the limit when n tends to infinity of the distance of the characteristic function χ of the interval $[1,+\infty[$ to the subspace generated by f_n ([2], [3]) is

$$\lim_{n\to\infty} d_n^2(\chi, f_n) = 1 - \frac{(1-\gamma)^2c^2 + 2c(1-\gamma)\alpha + \alpha^2}{c^2(\log 2\pi - \gamma) + 2c\lambda + \beta}$$

By means of Báez-Duarte criterion [1] the Riemann hypothesis holds if

$$\left(\log 2\pi + \gamma - \gamma^2 - 1\right)c^2 + 2\left(\lambda - (1-\gamma)\alpha\right)c + \beta - \alpha^2 = 0.$$

This expression is an equation of second degree on c and it's discriminant Δ' is only negative. If $\Delta' = 0$ we get $c = \frac{(1-\gamma)\alpha-\lambda}{\log 2\pi-\gamma-(1-\gamma)^2}$.

References

[1] L. Báez-Duarte, News versions of the Nyman-Beurling criterion for the Riemann hypothesis, *Int. J. Math. Math. Sci.* Vol. 31, Issue 7, (2002), pp.387-406.

[2] A. Bayad, M. Goubi, Proof of the Möbius conjecture revisited, *Proc. Jangjeon Math. Soc.*, Vol. 16 (2013), No. 2, pp. 237-243.

[3] M. Goubi, A. Bayad and M.O. Hernane, Explicit and asymptotic formulae for Vasyunin-Cotangent sums, *Pub. Inst. Math.*, Vol. 102 (2017) 116, pp. 155-174.

Goubi Mouloud
department of Mathematics, UMMTO university,
15000 Tizi-ouzou Algeria.
email: mouloud.ummto@hotmail.fr

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 4, *Number* 1, *March* 2019, *pages* 137-138

Computing isomorphism classes of abelian varieties over finite fields

Stefano Marseglia

Deligne proved in [Del69] that the category of ordinary abelian varieties over a finite field $\mathbb{F}_q$ is equivalent to the category of free finitely generated $\mathbb{Z}$-modules endowed with an endomorphism satisfying certain easy-to-state axioms. In [CS15] Centeleghe and Stix extended this equivalence to all isogeny classes of abelian varieties over whose characteristic polynomial of Frobenius does not have real roots under the assumption that q is a prime number. Let C be an isogeny class in source category of Deligne or Centeleghe-Stix' equivalences and let h be the Weil polynomial associated to C. Assume that h is square-free and denote by K the $\mathbb{Q}$-algebra $\mathbb{Q}[x]/(h)$. Put $F = x \bmod h$ and $V = q/V$ and consider the order $R = \mathbb{Z}[F, V]$ in K. Using Deligne's and Centeleghe-Stix' equivalences we obtain the following:

Theorem 1 *[Mar18b] There is an equivalence between the category of abelian varieties in C and the category of fractional R-ideals in K.*

In particular, we get a bijection between the isomorphism classes of abelian varieties in C and the *ideal class monoid* of R. There are well known algorithms to compute the group of invertible ideal classes of an order but not much can be found in the literature about non-invertible ideals. In [Mar18a] we explain how to effectively compute

representatives of all ideal classes for any order in a product of number fields, allowing us to compute the isomorphism classes of the abelian varieties in C. Moreover, using results of Howe from [How95], in the ordinary case we are able to translate the notion of dual variety, polarizations and automorphisms (of the polarized abelian variety) in the category of fractional R-ideal and we provide algorithms to compute them, see [Mar18b].

References

[CS15] Tommaso Giorgio Centeleghe and Jakob Stix, *Categories of abelian varieties over finite fields, I: Abelian varieties over* $\mathbb{F}_p$, Algebra Number Theory **9** (2015), no. 1, 225–265.

[Del69] Pierre Deligne, *Variétés abéliennes ordinaires sur un corps fini*, Invent. Math. **8** (1969), 238–243.

[How95] Everett W. Howe, *Principally polarized ordinary abelian varieties over finite fields*, Trans. Amer. Math. Soc. **347** (1995), no. 7, 2361–2401.

[Mar18a] Stefano Marseglia, *Ideal class monoid of an order and conjugacy classes of integral matrices*, arXiv:1805.09671.

[Mar18b] Stefano Marseglia, *Computing isomorphism classes of square-free polarized abelian varieties over finite fields*, arXiv:1805.10223. 2018.

Stefano Marseglia
Matematiska Institutionen
Stockholms Universitet
Kräftriket
106 91, Stockholm, Sweden.
email: stefanom@math.su.se

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 4, *Number* 1, *March* 2019, *pages* 139-140

Reductions of elliptic curves

Antonella Perucca

This is joint work with Davide Lombardo [3] and Peter Bruin [1]. The problem under consideration can be formulated for connected commutative algebraic groups, and our main results hold for all products of abelian varieties and tori. For simplicity, we focus here on the case of elliptic curves and present a selection of the results.

Let E be an elliptic curve defined over a number field K, and fix some prime number ℓ. Let $\alpha \in E(K)$ be a point of infinite order and consider the primes $\mathfrak{p}$ of K for which the reduction of α modulo $\mathfrak{p}$ is well-defined and has order coprime to ℓ. The aim of this paper is understanding the natural density $\mathrm{Dens}_\ell(\alpha)$ of this set (which is known to exist).

In [2], Jones and Rouse considered the Galois action on the tree of ℓ^∞ division points over α, which encodes the Kummer representation for α and the ℓ-adic representation attached to E. By refining their method, we are able to remove all assumptions and prove:

Theorem 1 *If $\mathcal{G}$ is the image of the ℓ-adic representation, we have*

$$\mathrm{Dens}_\ell(\alpha) = \mathrm{c}_{Kummer} \cdot \int_{\mathcal{G}} \ell^{-v_\ell(\det(x-I))} \cdot \mathrm{w}(x)\ d\mu_{\mathcal{G}}(x),$$

where $\mu_{\mathcal{G}}$ is the normalized Haar measure on $\mathcal{G}$, where the rational number c_{Kummer} measures the failure of maximality for the Kummer extensions of α, and where the function w *describes the Galois action*

on the tree of ℓ^∞ division points over α (its values can be either zero or a power of ℓ with exponent in $\mathbb{Z}_{\leq 0}$).

With different techniques we prove a completely new result:

Theorem 2 *The density* $\mathrm{Dens}_\ell(\alpha)$ *is a rational number (strictly between* 0 *and* 1*), and there is a theoretical algorithm that computes it. The minimal denominator of* $\mathrm{Dens}_\ell(\alpha)$ *divides, up to a power of* ℓ*, the expression* $(\ell-1)(\ell^2-1)^2(\ell^{12}-1)$.

The power of ℓ in the minimal denominator of $\mathrm{Dens}_\ell(\alpha)$ cannot be uniformly bounded, therefore we give a bound depending on α.

We also generalize the above results by replacing ℓ with a (square-free) integer m.

References

[1] P. Bruin and A. Perucca, *Reductions of points on algebraic groups II*, submitted for publication.

[2] R. Jones and J. Rouse, *Iterated endomorphisms of abelian algebraic groups*, Proc. Lond. Math. Soc. (3) **100** (2010), no. 3, 763–794.

[3] D. Lombardo and A. Perucca, *Reductions of points on algebraic groups*, submitted for publication.

Antonella Perucca
Mathematics Research Unit
University of Luxembourg
6, av. de la Fonte
4364 Esch-sur-Alzette, Luxembourg.
email: antonella.perucca@uni.lu

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 4, *Number* 1, *March* 2019, *pages* 141-142

Non-Wieferich primes and Euclidean algorithm in number fields

Srinivas Kotyada and
Subramani Muthukrishnan

An odd prime p is said to be a non-Wieferich prime with respect to the base a if

$$a^{p-1} \not\equiv 1 \pmod{p^2}. \tag{1}$$

The following are some important results on non-Wieferich primes.

Theorem 1 *(J.H. Silverman [1]) For any fixed $\alpha \in \mathbb{Q}^{\times}, \alpha \neq \pm 1$, and assuming the abc conjecture, card $\left\{p \leq x : \alpha^{p-1} \not\equiv 1 \pmod{p^2}\right\} \gg_{\alpha} \log x$ as $x \to \infty$.*

Theorem 2 *(M. Ram Murty, H. Graves [2]) For any $a \geq 2$ and any fixed $k \geq 2$, there are $\gg \log x/\log\log x$ primes $p \leq x$ such that $a^{p-1} \not\equiv 1 \pmod{p^2}$ and $p \equiv 1 \pmod{k}$, under the assumption of abc conjecture.*

Recently, the authors generalized the notion of non-Wieferich primes to algebraic number fields [3] and proved the following theorems.

Theorem 3 *[3] Let $K = \mathbb{Q}(\sqrt{m})$ be a real quadratic field of class number one and assume that the abc conjecture holds true in K. Then there are infinitely many non-Wieferich primes in O_K with respect to the unit ε satisfying $|\varepsilon| > 1$.*

Theorem 4 *[3] Let K be any algebraic number field of class number one and assume that the abc conjecture holds true in K. Let η be a unit in O_K satisfying $|\eta| > 1$ and $|\eta^{(j)}| < 1$ for all $j \neq 1$, where $\eta^{(j)}$ is the jth conjugate of η. Then there exist infinitely many non-Wieferich primes in K with respect to the base η.*

By computing non-Wieferich primes in number fields the authors proved that certain cyclic cubic fields of class number one are Euclidean (see [4] for details).

References

[1] J. H. Silverman *Wieferich's criterion and the abc-conjecture,* J. Number Theory. 30 (1988), no. 2, 226 – 237.

[2] H. Graves, M. Ram Murty, *The abc conjecture and non-Wieferich primes in arithmetic progressions,* J. Number Theory 133 (2013), 1809 –1813.

[3] K. Srinivas, M. Subramani, *Non-Wieferich primes in number fields and abc conjecture*, Czechoslovak Mathematical Journal, 68, no. 2, 2018, 445-453.

[4] K. Srinivas, M. Subramani, *A note on Euclidean cyclic cubic fields.* JRMS, 33, vol.2, 2018, 125-133.

Srinivas Kotyada
Professor, Institute of Mathemcmical Sciences
HBNI, CIT Campus, Taramani
Chennai - 600 113, India.
email: srini@imsc.res.in

Subramani Muthukrishnan
Harish Chandra Research Institute, HBNI
Chhatnag Road, Allahabad - 211 019, India.
email: msubramani@hri.res.in

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 4, *Number* 1, *March* 2019, *pages* 143-145

Conjectural estimates on the Mordell-Weil and the Tate-Shavarevich groups of an abelian variety

Andrea Surroca Ortiz

The Mordell-Weil theorem states that the group of rational points $A(K)$ on an Abelian variety A defined over a number field K is finitely generated: $A(K) \simeq A(K)_{\text{tors}} \oplus \mathbb{Z}P_1 \oplus \ldots \oplus \mathbb{Z}P_r$. While there exist results on the torsion part, the free part remains less tractable. Even in the particular case of an elliptic curve, there is no way, in general, to compute the rank r or a set of generators $\{P_i\}_{i=1,\ldots,r}$ of this group.

The proof of the Mordell-Weil theorem involves the Tate-Shafarevich group $Ш(A/K)$ of A/K, which measures the obstruction to the Hasse principle. Even if it is not easy to construct a non trivial element of this group, it is still unknown, in the general case, if it is finite.

For some applications, it would be sufficient to bound the "size" of the invariants of the variety. We explore here how could be bounded

1- the product $|Ш(A/K)| \cdot \text{Reg}(A/K)$ of the order of $Ш(A/K)$ and the canonical regulator,

2- the canonical height $\hat{h}_{\mathcal{L}}(P_i)$ of a well chosen system of generators of the free part of $A(K)$, as well as

3- the order $|Ш(A/K)|$ of the Tate-Shafarevic group.

Our bounds are implied by strong but nowadays classical conjectures. We follow the approach of Manin, who proposed a conditional algorithm for finding a basis for the non-torsion rational points of an elliptic curve over $\mathbb{Q}$. We **e**xtend Manin's method to an Abelian variety of arbitrary dimension, defined over an arbitrary number field. Our bounds are **e**xplicit in all the parameters: the Faltings' height $h = h_{Falt}(A/K)$ (which measures the arithmetic complexity of the variety), the absolute value $\mathcal{F} = |N_{K/\mathbb{Q}}\mathcal{F}_{A/K}|$ of the norm of the conductor (which gives information about the places of bad reduction), the dimension g of A, the Mordell-Weil rank $r = \mathrm{rk}(A(K))$, the degree $d = [K : \mathbb{Q}]$, and the absolute value D_K of the discriminant of K.

In this work,

- with point 1, we refine a conjecture of Hindry (related works in different settings have been done also by Hindry-Pacheco and Griffon), and extend to the general case of A/K,

- with point 2, a conjecture of Lang, for elliptic curves over $\mathbb{Q}$,

- with point 3, a result by Goldfeld and Szpiro, towards their conjecture $|Ш(E/K)| = O(\mathcal{F}_{E/K}^{1/2+\epsilon})$. Furthermore, we **i**mprove their result in the one dimensional case over the field of rational numbers.

The method is based on the Hasse-Weil conjecture which suppose that the L-series of A has an analytic continuation to $\mathbb{C}$ and satisfies a functional equation at 1, and on the Birch-Swinnerton-Dyer conjecture, which translates analytic information into geometric and arithmetic information. We suppose that $|Ш(A/K)|$ is finite, and conclude with Minskowski's theorem, since the Néron-Tate pairing relates the regulator to the volume of the fundamental domain of the lattice $A(K)/A(K)_{\mathrm{tors}}$.

Andrea Surroca Ortiz
4, rue Beethoven
67000 Strasbourg, France.
email: andrea.surroca.o@gmail.com