Proceedings of the 2nd mini symposium of the Roman Number Theory Association

Università Roma Tre

April 26th, 2016

Contents

Foreword

This volume contains the proceedings of the second mini symposium of the Roman Number Theory Association. The conference was held on April 26, 2015 at the Università degli Studi Roma Tre. As organizers of the symposium, and promoters of the association, we would like to thank the speakers for the high scientific contribution offered, and the "scribas" who wrote these notes. We also thank the Università Europea di Roma and the Università Roma Tre for funding the event.

The Roman Number Theory Association

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

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

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

Our statute is available on the association's website (www.rnta.eu) and it clearly states that our efforts and our funds will be devoted entirely to the development of Number Theory. This will be achieved in several ways: by directly organising events - an annual symposium in Rome as well as seminars distributed over the year; by participating and supporting, both scientifically and financially, workshops, schools and conferences on the 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 Mini Symposium, was slightly different. In the weeks before the symposium, we identified a list of PhD students and young researchers to whom we proposed to carry out a particular task: that one of the "scriba". Each young scholar was then paired with one of the speakers and was asked to prepare a written report on the talk of the speaker he was assigned to. Of course in doing so the scribas had to get in contact with speakers after the conference in order to get the needed bibliographical references as well as some insight on the topic in question. We would like to highlight that both the speakers and scribas joined the project enthusiastically.

The reasons for this choice lies in the most essential aim of our Association: introducing young researchers to number theory, in all its possible facets. The benefits of this project were twofold: on one hand, the "scribas" had to undertake the challenging task of writing about a topics different from their thesis or their first article subject

and learn about a new possible topic of research and, on the other, they had the possibility to collaborate with a senior researcher and learn some trick of the trade.

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

Report on RNTA Activities

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

The Third mini Symposium of the association will take place on the 6th of April 2017; for us this is a very special moment since it will bring together most people involved in RNTA and especially our Advisory Board. The proceedings of the first two symposia have been published, and the scriba project has been already launched for the third one.

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

- *The Tenth International Conference on Science and Mathematics Education in Developing Countries*, Mandalay University, Myanmar, to be held in November 2017.
- *Symposium for South Asian Women in Mathematics*, Tribhuvan University (TU), Kathmandu, Nepal, to be held in October 13th - 15th, 2017;
- *Ninth International Conference on Science and Mathematics Education in Developing Countries*, Mandalay University, Mandalay, The Republic of the Union of Myanmar, held in November 4-6, 2016;
- *Leuca 2016, Celebrating Michel Waldschmidt's 70th birthday*, Marina di San Gregorio, Patù (Lecce, Italy) held in June 13 - 17, 2016.

LEUCA2016 - GROUP PICTURE

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

- CIMPA research school on *Arithmétique algorithmique et cryptographie*. Université de Kinshasa, Kinshasa, Democratic Republic of Congo, to be held in May 7 - 18, 2018.
- CIMPA research school on *Explicit Number Theory*, The Witwatersrand University, Johannesburg, South Africa, to be held in 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, to be 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, to be held in April 10-22, 2017;

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

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

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

The Association also supports the *Nepal Algebra Project*. This is consist of 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. In each of the six years one course of 50 hours will be offered at Tribhuvan University by several lecturers from developed countries.

The course lasts 10 weeks (five hours each week) . It is divided into five modules, each of two weeks. Every module is taught by a different lecturer according to a rigid schedule.

NAP2016 - GROUP PICTURE ON THE FINAL EXAM DAY

MARINA MONSURRÒ, UNIVERSITÀ EUROPEA DI ROMA
email: marina.monsurro@unier.it

FRANCESCO PAPPALARDI, DIPARTIMENTO DI MATEMATICA E FISICA, UNIVERSITÀ ROMA TRE
email: pappa@mat.uniroma3.it

VALERIO TALAMANCA, DIPARTIMENTO DI MATEMATICA E FISICA, UNIVERSITÀ ROMA TRE
email: valerio@mat.uniroma3.it

ALESSANDRO ZACCAGNINI, DIPARTIMENTO DI SCIENZE MATEMATICHE, FISICHE ED INFORMATICHE, UNIVERSITÀ DI PARMA
email: alessandro.zaccagnini@unipr.it

OFFICIAL PHOTO and PARTICIPANTS LIST

1. Marco Cantarini (Università di Parma)
2. Mohammed Anwar (Università Roma Tre)
3. Filippo Viviani (Università Roma Tre)
4. Alessandro Zaccagnini (Università di Parma)
5. Andreas Bender (Università di Pavia)
6. Edmond Comlan Koudjinan (Università Roma Tre)
7. Valerio Talamanca (Università Roma Tre)
8. Fabio Caldarola (Università della Calabria)
9. Corrado Falcolini (Università Roma Tre)
10. Federico Campanini (Università Roma Tre)
11. Lorenzo Menici (Università Roma Tre)
12. Nilakantha Paudel (Università Roma Tre)
13. Marco Pedicini (Università Roma Tre)
14. Carlo Sanna (Università di Torino)
15. Leonardo Cangelmi (Università G. D'Annunzio Chieti Pescara)
16. Francesco Pappalardi (Università Roma Tre)
17. Chaohua Jia (Chinese Academy of Sciences, Beijing)
18. Christian Maire (Université de Franche Compte)
19. Pietro Mercuri (Università di Roma Tor Vergata)
20. Shigeru Kanemitsu (Kinki University)

21. Pierfrancesco Carlucci (Università Tor Vergata)
22. Michel Walschmidt (Université Pierre et Marie Curie)
23. Louis Nantenaina Andrianaivo (Università Roma Tre)
24. Leo Murata (Meiji Gakuin University)
25. Marina Monsurrò (Università Europea di Roma)

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 2, *Number* 1, *March* 2017, *pages* 1-12

Michel Waldschmidt

Some Results on Diophantine equations

Written by Louis Nantenaina Andrianaivo

1 Introduction

Let $k \in \mathbb{Q}$, $k \neq 0$, $d \geq 3$ a positive integer and consider an irreducible bivariate form $F(X,Y) = \sum_{i=1}^{d} a_i X^{d-i} Y^i \in \mathbb{Z}[X,Y]$. In 1908, Axel Thue initiated the study of the Diophantine equations of the form $F(X,Y) = k$; this is the reason why they are called **Thue Equations**. Thue obtained one fundamental theorem:

Theorem 1 (Thue 1908) *Let $F \in \mathbb{Z}[X,Y]$ be a homogeneous irreducible form of degree $d \geq 3$:*

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

Let $k \in \mathbb{Z}$, $k \neq 0$. Then there are only finitely many integer solutions $(X,Y) \in \mathbb{Z} \times \mathbb{Z}$ of the Diophantine equation $F(X,Y) = k$.

Since then, the above theorem has been improved by many mathematicians. In this exoposition, we concentrate on the family constructed by E.Thomas, and later generalized by C. Levesque and M. Waldschmidt. One of the first result in diophantine apporximantion si:

Theorem 2 (Liouville's inequality 1844) *Let α be an algebraic number of degree $d \geq 2$. There exists $c(\alpha) > 0$ such that, for any $\frac{p}{q} \in \mathbb{Q}$ with $q > 0$,*

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

The inequality of Theorem 2 can be improved for algebraic numbers α of degree $d > 2$. In fact the exponent d in the denominator is best possible for $d = 2$ but it is not for $d \neq 3$. In 1909, Thue proved the following theorem:

Theorem 3 (Thue 1909) *Let α be an algebraic number of degree $d > 2$ and let $\kappa > (\frac{d}{2}) + 1$. Then there exists $c(\alpha, \kappa) > 0$ such that, for any $\frac{p}{q} \in \mathbb{Q}$ with $q > 0$,*

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

Later, the exponent κ in the denominator above has been improved:

1921: C.L. Siegel, with $\kappa = 2\sqrt{d}$;

1947: F.J. Dyson and A.O. Gel'fond; with $\kappa = \sqrt{2d}$

1955: K.F. Roth, with any $\kappa > 2$.

There is a close relation between the finiteness of the number of solutions of the Thue's equation and approximation of rational numbers. For example in [2] one can find the proof of the following:

Theorem 4 *Let $f \in \mathbb{Z}[X]$ be an irreducible polynomial of degree d and let $F(X, Y) = Y^d f(X/Y)$ be the associated homogeneous binary form of degree d. Then the following two assertions are equivalent:*
(i) For any $k \in \mathbb{Z}^\times$, $F(X, Y) = k$ has only finitely many solutions in $\mathbb{Z}^2$
(ii) For any real number $\kappa > 0$ and for any root $\alpha \in \mathbb{C}$ of f, there are only finitely many rational number $\frac{p}{q}$ such that

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

Note that (i) can be rephrased as:
For any positive integer $k \neq 0$, the set of $(X, Y) \in \mathbb{Z}^2$ verifying

$$0 < |F(X, Y)| \leq k.$$

is finite. Also, for any number field K, for any non-zero element $k \in K$ and for any elements $\alpha_1, \ldots, \alpha_n \in K$ with $\mathrm{Card}\{\alpha_1, \ldots, \alpha_n\} \geq 3$, the Thue equation

$$(X - \alpha_1 Y) \cdots (X - \alpha_n Y) = k.$$

has only a finite number of solutions $(X, Y) \in \mathbb{Z} \times \mathbb{Z}$.
Now, one will describe some approach which has been used to deal with Thue equations and discuss a further results related on it.

Theorem 5 (Schmidt's Subspace Theorem 1970) *Let $L_0, \ldots, L_{m-1}$ be $m \geq 2$ independent linear forms in m variables with algebraic coefficients. Let $\epsilon > 0$. Then the set*

$$\{X = (X_0, \ldots, X_{m-1}) \in \mathbb{Z}^m : |L_0(X) \cdots L_{m-1}(X)| \leq |X|^{-\epsilon}\}.$$

is contained in the union of finitely many proper subspaces of $\mathbb{Q}^m$.

One can use the above theorem to prove the following celebrated result:

Theorem 6 (Thue, Siegel and Roth) *For any real algebraic number α, and for any $\epsilon > 0$, there are only finitely many $o\frac{p}{q} \in \mathbb{Q}$ with $q > 0$ such that*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{2+\epsilon}}.$$

In fact, the proof of Thue-Siegel-Roth Theorem can be used to produce an upper bound of the number of solutions of a Diophantine equation in the above family, but no upper bound for the sizes of solutions can be derived. R. Baker and N. I. Fel'dman developed an effective method introduced by A.O. Gel'fond, involving lower bounds for linear combinations of logarithms of algebraic numbers with algebraic coefficients.

Since $e^z - 1 \sim z$ for $z \longrightarrow 0$, determining lower bounds for the following two non-vanishing numbers is equivalent:

$$\alpha_1^{b_1} \cdots \alpha_n^{b_n} - 1 \qquad\qquad b_1 \log \alpha_1 + \cdots + b_n \log \alpha_n.$$

The first nontrivial lower bounds were obtained by A.O. Gel'fond. His estimates were effective only for $n = 2$; for $n \geq 3$, he needed to use estimates related to the Thue-Siegel-Roth Theorem.

In 1968, A. Baker succeeded to extend to any $n \geq 2$ the transcendence method used by A.O. Gel'fond for $n = 2$. As a consequence, effective upper bounds for the solutions of Thue's equations have been derived.

In the same year, A. Schinzel computed explicitly the constants introduced by A.O. Gel'fond in his lower bound for $|\alpha_1^{b_1}\alpha_2^{b_2} - 1|$.

The approach for solving Thue equations, given by Gel'fond and Baker, is based on the exploitation of Siegel's unit equation: assume $\alpha_1, \alpha_2, \alpha_3$ are algebraic integers and X, Y rational integer such that:$(X - \alpha_1 Y)(X - \alpha_2 Y)(X - \alpha_3 Y) = 1$. The elements $u_1 = X - \alpha_1 Y\,, u_2 = X - \alpha_2 Y\,, u_3 = X - \alpha_3 Y$ are units. By eliminating X and Y in the three linear relations above, we obtain

$$u_1(\alpha_2 - \alpha_3) + u_2(\alpha_3 - \alpha_1) + u_3(\alpha_1 - \alpha_2) = 0.$$

We write it as a Siegel's unit equation in the form

$$\frac{u_1(\alpha_2 - \alpha_3)}{u_2(\alpha_1 - \alpha_3)} - 1 = \frac{u_3(\alpha_2 - \alpha_1)}{u_2(\alpha_1 - \alpha_3)}\cdot$$

By identifying, the quantity $\alpha_1^{b_1} \cdots \alpha_n^{b_n}$ in Gel'fond-Baker Diophantine inequality with the quotient $\dfrac{u_1(\alpha_2 - \alpha_3)}{u_2(\alpha_1 - \alpha_3)}\cdot$, one can then apply the theory of Siegel's unit equations.

2 Families of Thue equations

There are several families of Thue equations which many mathematicians tried to solve. The first family of Thue equation was given by Thue himself:

$$(a + 1)X^n - aY^n = 1.$$

For n prime and a sufficiently large in term of n (for instance, $n = 3$ and for $a \geq 386$), the only one solution in positive integers X, Y is $X = Y = 1$.
E. Thomas considered the family of the Thue equations $F_n(x, y) = \pm 1$ where $F_n(X, Y) = X^3 - (n-1)X^2Y - (n+2)X - Y^3$. In 1990, he proved in some effective way that the set of $(X, Y, n) \in \mathbb{Z}^3$ such that $n \geq 0$, $\max\{|x|, |y|\} \geq 2$, and $F_n(x, y) = \pm 1$ is finite. In [4] he completely solved the equation $F_n(X, Y) = 1$, for $n \geq 1.365 \cdot 10^7$; the only solutions are $(0, -1)$, $(1, 0)$ and $(-1, 1)$.

D. Shanks introduced the simplest cubic fields $\mathbb{Q}(\lambda)$ by studying the field $\mathbb{Q}(\omega)$ where ω is a solution of

$$F_n(X, 1) = X^3 - (n-1)X^2 - (n+2)X - 1. \tag{1}$$

He proved that if λ is one of the solutions of equation (1), then $\mathbb{Q}(\lambda)$ is a real Galois field.

In 1993, M. Mignotte [5] completed this result by solving this equation for each n. For $n \geq 4$ and for $n = 2$, the only solutions to $F_n(X, Y) = 1$ are $(0, -1)$, $(1, 0)$ and $(-1, 1)$.
M. Mignotte worked with A. Lethö and F. Lemmermeyer. In 1996, they studied, in [6], the family of Diophantine equations $F_n(X, Y) = k$, for $k \neq 0$. They obtained the following theorem,

Theorem 7 (Mignotte, Pethö and Lemmermeyer 1996) *For $n \geq 2$, when X, Y are rational integers verifying*

$$0 < |F_n(X, Y)| \leq k \quad (k \in \mathbb{Z})$$

then

$$\log|y| < c(\log n)(\log n + \log k).$$

with an effectively computable absolute constante c.

When k is a given positive integer, there exists an integer n_0 depending upon k such that $|F_n(X, Y)| \leq k$ with $n \geq 0$ and $|Y| > \sqrt[3]{k}$ implies $n \leq n_0$. But, for $0 \leq |t| \leq \sqrt[3]{m}$, $(-t, t)$ and $(t, -t)$ are solutions, therefore

the condition $|Y| > \sqrt[3]{k}$ cannot be omitted.
Note that Theorem 7 gives an upper bound for $\max\{|x|, |y|\}$ which depends on k and n while we would like a bound only depending on k.
We now come to the main goal of this work: presenting Claude Levesque and Michel Waldschmidt' s approach for solving families of diophantine Thue equation. In 2010, C. Levesque proposed to consider the following version Thomas's family of cubic Thue equations:

$$F_{n,2}(X, Y) = (X - \lambda_{0n}^2 Y)(X - \lambda_{1n}^2 Y)(X - \lambda_{2n}^2 Y).$$

where λ_{in} are units in the totally real cubic field $\mathbb{Q}(\lambda_{0n})$. The natural question was: Does Thomas result hold?
Given any irreducible binary form $F \in \mathbb{Z}[X, Y]$, α a root of $F(X, 1)$, and ϵ a unit in the field $\mathbb{Q}(\alpha)$, consider the family of Diophantine equations, $F_a(X, Y) = k$, $(a \in \mathbb{Z})$, where $F_a(X, Y)$ is deduced from $F(X, Y) = \prod_{i=1}^{d}(X - \sigma_i(\alpha)Y)$, by twisting with ϵ^a, assuming $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha\epsilon^a)$. Here $F_a(X, 1)$ is the irreducible polynomial of $\alpha\epsilon^a$ and

$$F_a(X, Y) = \prod_{i=1}^{d}(X - \sigma_i(\alpha\epsilon^a)Y).$$

By using Schmidt's subspace theorem, their first result was: Given α to be an algebraic number of degree $d \geq 3$ and K=$\mathbb{Q}(\alpha)$. Let ϵ be a unit of K such that $\alpha\epsilon$ has degree d, $f_\epsilon(X)$ be the irreducible polynomial of $\alpha\epsilon$ and $F_\epsilon(X, Y)$ be its homogeneous version. Then for all but finitely many of these units, the Thue equation $F_\epsilon(X, Y) = \pm 1$ has only the trivial solution X, Y in $\mathbb{Z}$ where $XY = 0$. Now, let consider

$$F_{n,a}(X, Y) = (X - \lambda_{0n}^a Y)(X - \lambda_{1n}^a Y)(X - \lambda_{2n}^a Y) \quad \in \mathbb{Z}[X, Y].$$

with a new parameter $a \in \mathbb{Z}$.

Q 1 *Are there only finitely many* (n, a, X, Y) *satisfying* $F_{n,a}(X, Y) = \pm 1$?

For the next result, we need the *absolute logarithmic height* h which is defined by $h(\alpha) = \frac{1}{d}\log M(\alpha)$ where M is the *Malher measure*

$$M(\alpha) = a_0 \prod_{1\leq i\leq d} \max\{1, |\sigma_i(\alpha)|\}$$

and a_0 is the leading coefficient of the irreducible polynomial of α over $\mathbb{Z}$.

In 2013, C. Levesque and M. Waldschmidt stated the following conjecture in [3].

Conjecture 1 (Levesque and Waldschmidt 2013) *There exists $\kappa > 0$, constant depending only on α, such that, for any $k \geq 2$, all solutions (X, Y, ϵ) in $\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}_k^\times$ of the inequality*

$$|F_\epsilon(X, Y)| \leq k, \text{ with } XY \neq 0 \text{ and } [\mathbb{Q}(\alpha\epsilon) : \mathbb{Q}] = 3,$$

satisfy

$$\max\{|X|, |Y|, e^{h(\alpha\epsilon)}\} \leq k^\kappa.$$

One year later, they proved the following theorem which is one of the main result presented here. The key point of the proof, is an approach for finding the upper bound for the solution which does not depend on n which we sketch below a complete proof can be found in [1].

Theorem 8 (Levesque and Waldschmidt 2014) *There is an effectively computable absolute constant $c > 0$ such that, if (X, Y, n, a) are nonzero rational integers with $\max\{|X|\,|Y|\} \geq 2$ and $F_{n,a}(x, y) = \pm 1$, then $\max\{|a|\,|n|, |X|\,|X|\} \leq c$. Furthermore, for all $n \geq 0$, the trivial solution with $a \leq 2$ are $(0, 1), (1, 0)$ and for $a = 2$ is $(1, 1)$.*

Proof. Let us write λ_i for λ_{in} for $i = 0, 1, 2$. Then

$$F_n(X, Y) = X^3 - (n-1)X^2Y - (n+2)XY^2 - Y^2.$$

can be written as $F_n(X, Y) = (X - \lambda_0 Y)(X - \lambda_1 Y)(X - \lambda_2 Y)$

so we have: $\begin{cases} n + \frac{1}{n} \leq \lambda_0 \leq n + \frac{2}{n}, \\ -\frac{1}{n+1} \leq \lambda_1 \leq -\frac{1}{n+2}, \\ -1 - \frac{1}{n} \leq \lambda_2 \leq -1 - \frac{1}{n+1}. \end{cases}$

- One defines $\gamma_i = X - \lambda_i^a Y$, $(i = 0, 1, 2)$, so $F_{n,a}(X, Y) = \pm 1$ becomes $\gamma_0\gamma_1\gamma_2 = \pm 1$. By writing γ_i to be γ_{i_0}, we have the bound $|\gamma_{i_0}| \leq \frac{m}{Y^2\lambda_0^a}$. Also we have $\min\{|\gamma_{i_1}|, |\gamma_{i_2}|\} > Y|\lambda_0^a|$.

- By considering the group of units of $\mathbb{Q}(\lambda_0)$, and taking λ_1, λ_2 as a base, there exist $\delta = \pm 1$ and rational integers A and B which verify

$$|A| + |B| \leq \kappa \left(\frac{\log Y}{\log \lambda_0} + a \right),$$

where, $\begin{cases} \gamma_{0,a} &= \delta\lambda_0^A\lambda_2^B, \\ \gamma_{1,a} &= \delta\lambda_1^A\lambda_0^B &= \delta\lambda_0^{-A+B}\lambda_2^{-A}, \\ \gamma_{2,a} &= \delta\lambda_2^A\lambda_1^B &= \delta\lambda_0^{-B}\lambda_2^{A-B}. \end{cases}$

- Transform the following Siegel unit equation,

$$\gamma_{i_0,a}(\lambda_{i_1}^a - \lambda_{i_2}^a) + \gamma_{i_1,a}(\lambda_{i_2}^a - \lambda_{i_0}^a) + \gamma_{i_2,a}(\lambda_{i_0}^a - \lambda_{i_1}^a) = 0,$$

as

$$\frac{\gamma_{i_1,a}(\lambda_{i_2}^a - \lambda_{i_0}^a)}{\gamma_{i_2,a}(\lambda_{i_1}^a - \lambda_{i_0}^a)} - 1 = -\frac{\gamma_{i_0,a}(\lambda_{i_{100}}^a - \lambda_{i_2}^a)}{\gamma_{i_2,a}(\lambda_{i_1}^a - \lambda_{i_0}^a)}\cdot$$

we have the estimate

$$0 < \left| \frac{\gamma_{i_1,a}(\lambda_{i_2}^a - \lambda_{i_0}^a)}{\gamma_{i_2,a}(\lambda_{i_1}^a - \lambda_{i_0}^a)} - 1 \right| \leq \frac{2}{Y^3\lambda_0^a}\cdot$$

At the end we have to separate two cases, first, when n is large, the completion of the proof is from the lower bound for a linear form in logarithms of algebraic numbers (Baker's method).
For n bounded, we have results which are valid for the family of Thue equations of Thomas and the completion of the proof follows from the following Lemma,

Lemma 1 *Consider a monic irreducible cubic polynomial* $f(X) \in \mathbb{Z}[X]$ *with* $f(0) = \pm 1$ *and write,*

$$F(X, Y) = Y^3 f(X/Y) = (X - \epsilon_1 Y)(X - \epsilon_2 Y)(X - \epsilon_3 Y).$$

For $a \in \mathbb{Z}$, $a \neq 0$, define

$$F_a(X,Y) = (X - \epsilon_1^a Y)(X - \epsilon_2^a Y)(X - \epsilon_3^a Y).$$

Then there exists an effectively computable constant $\kappa > 0$ depending only on f, such that, for any $k \geq 2$, any (x, y, a) in the set

$$\left\{(X,Y,a) \in \mathbb{Z}^2 \times \mathbb{Z} \mid XYa \neq 0, \max\{|X|,|Y|\} \geq 2, F_a(X,Y) \leq k\right\}$$

satisfies $\max\{|X|,|Y|,e^{|a|}\} \leq k^\kappa$. □

In 2015, further results were proved in [1]. The following is one of those.

Theorem 9 (Levesque and Waldschmidt 2015) *Let $k \geq 1$. There exists an absolute effectively computable constant κ such that, if there exists $(n, a, k, X, Y) \in \mathbb{Z}^2$ with $a \neq 0$ verifying $0 < |F_{n,a}(X,Y)| \leq k$,*

- *then*
$$\log\{|X|,|Y|\} \leq \kappa\mu.$$
with $\mu = \begin{cases} (\log k + |a|\log|n|)(\log|n|)^2 \log\log|n| & \text{for } |n| \geq 3, \\ \log k + |a| & \text{for } |n| \leq 2. \end{cases}$
Note that if $a = 1$, this follows from Theorem 7.

- *if $n \geq 0$, $a \geq 1$ and $|y| \geq 2\sqrt[3]{k}$, then $a \leq \kappa\mu'$ with*
$\mu' = \begin{cases} (\log k + \log n)(\log n)\log\log n & \text{for } |n| \geq 3, \\ 1 + \log k & \text{for } n = 0, 1, 2. \end{cases}$

- *if $XY \neq 0$ and $n \geq 0$ and $a \geq 1$, then*
$$a \leq \kappa \max\left\{1, (1 + \log|X|)\log\log(n+3), \log|Y|, \frac{\log k}{\log(n+2)}\right\}.$$

References

[1] Claude Levesque and Michel Waldschmidt, *A family of Thue equations involving powers of units of the simplest cubic fields*, 2015.
http://arxiv.org/abs/1505.06708

[2] Claude Levesque and Michel Waldschmidt, *Some remarks on diophantine equations and diophantine approximation*, 2013.
http://arxiv.org/abs/1312.7200

[3] Claude Levesque and Michel Waldschmidt, *Solving effectively some families of Thue Diophantine equations*, 2013.
http://arkiv.org/1312.7205

[4] Emery Thomas, *Complete solutions to a family of cubic Diophantine equations*, Journal of Number Theory, **34**, 235–250, 1990.

[5] Maurice Mignotte, *Verification of a Conjecture of E. Thomas*, Journal of Number Theory, **44**, 172–177, 1993.

[6] Maurice Mignotte, Attila Pethő and Franz Lemmermeyer, *On the family of Thue equations* $x^3-(n-1)x^2y-(n+2)xy^2-y^3 = k$, Acta Arithmetica, **76**, 245–269, 1996.

Louis Nantenaina Andrianaivo
Dipartimento di Matematica e Fisica
Università degli studi Roma Tre.
Largo S. L. Murialdo, 1
00146, Roma, Italy.
email: landrianaivo@mat.uniroma3.it

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 2, *Number* 1, *March* 2017, *pages* 11-20

Chaohua Jia

Kloosterman sums and shifted character sums with multiplicative coefficients

Written by Mohamed Anwar

1 Introduction on Kloosterman sum

Given a real number t, we write $e(t) = e^{2\pi i t}$. The sum

$$S(a,\, b;\, q) = \sum_{\substack{x=1 \\ (x,\, q)=1}}^{q} e\Big(\frac{ax + b\bar{x}}{q}\Big)$$

where $\bar{x}$ satisfies $\bar{x}x \equiv 1 \pmod q$, and is unique modulo q, is called a Kloosterman sum. Kloosterman sum play an important role in number theory. There is systematic and deep study on this type of sums. Kloosterman introduced this type of sums as early as 1926. His purpose was to study positive integer solutions of the quadratic diagonal form

$$N = a_1 n_1^2 + a_2 n_2^2 + a_3 n_3^2 + a_4 n_4^2,$$

where a_i are fixed positive integers. This problem is a generalization of Lagrange four squares theorem, the purpose of which is to determine for which coefficients $(a_1,\, a_2,\, a_3,\, a_4)$, all sufficiently large N can be

expressed in this form. Now it is difficult to apply Hardy-Littlewood circle method directly, and Kloosterman had to make an improvement on the circle method. During the proof he met the sum

$$\sum_{\substack{x=1\\(x,\,q)=1}}^{X} e\Big(\frac{b\bar{x}}{q}\Big),$$

which is called an incomplete Kloosterman sum.

If $(b,\,q)=1$, $X=q$, the above sum is a Ramanujan sum

$$\sum_{\substack{x=1\\(x,\,q)=1}}^{q} e\Big(\frac{b\bar{x}}{q}\Big) = \sum_{\substack{y=1\\(y,\,q)=1}}^{q} e\Big(\frac{y}{q}\Big) = \mu(q).$$

The incomplete sum can be transformed to a complete sum by a standard technique. Therefore

$$\Big|\sum_{\substack{x=1\\(x,\,q)=1}}^{X} e\Big(\frac{b\bar{x}}{q}\Big)\Big| \le (1+\log q)\max_{1\le a\le q}|S(a,\,b;\,q)|.$$

Now the problem is changed into finding an estimate for $S(a,\,b;\,q)$.

This sum can be traced back to a work of H. Poincaré in 1911. It is named after Kloosterman since he gave a non-trivial estimate for this sum for the first time. From now on we restrict to prime number $p=q$ in the treatment of Kloosterman sums. Firstly he considered the mean value

$$\sum_{r=0}^{p-1}\sum_{s=0}^{p-1}|S(r,\,s;\,p)|^4.$$

This mean value has an arithmetic meaning, i.e. is the number of solutions of the equation system

$$x_1+x_2-x_3-x_4\equiv 0, \qquad \bar{x}_1+\bar{x}_2-\bar{x}_3-\bar{x}_4\equiv 0\,(\mathrm{mod}\,p).$$

By an elementary discussion, the number of solutions does not exceed $3p^3(p-1)$.

Then for the fixed $a,\ b,\ p \nmid b$, there are at least $p-1$ terms $|S(a,\ b;\ p)|^4$ in the above mean value. Combining all of the above, we get

$$|S(a,\ b;\ p)| < 3^{\frac{1}{4}} p^{\frac{3}{4}}, \qquad p \nmid b.$$

This shows that in the above incomplete Kloosterman sum, if $X > p^{\frac{3}{4}+\varepsilon}$, there is some cancellation. By this estimate, Kloosterman can solve the problem on the quadratic diagonal form in four variables.

In 1948, Weil proved a stronger result

$$|S(a,\ b;\ p)| \leq 2p^{\frac{1}{2}}, \qquad p \nmid b,$$

which is a corollary of his proof of Riemann Hypothesis for curves in finite fields. This estimate is almost best possible, and is used in many applications of Kloosterman sum.

2 Applications

1) It is conjectured that every sufficiently large integer $N \equiv 4 \pmod{24}$ can be expressed as

$$N = p_1^2 + p_2^2 + p_3^2 + p_4^2,$$

where p_i is prime number. This is a development of Lagrange four squares theorem. The case for five primes was solved by L. Hua. The case for four primes is very difficult. In 1994, Brüdern and Fouvry proved that every sufficiently large integer $N \equiv 4 \pmod{24}$ can be expressed as

$$N = P_1^2 + P_2^2 + P_3^2 + P_4^2,$$

where the number of prime factors of every P_i is at most 34. In the proof, the improvement on circle method by Kloosterman and the

estimate for Kloosterman sum were used. Yingchun Cai improved the number 34 to 13. Recently Lilu Zhao improved it to 5.

2) Let p be prime, $(a,\ p) = 1$. Solve

$$mn \equiv a \pmod{p},$$

where positive integers m and n are small as possible.

Write $M(a)$ as the minimum of $\max(m,\ n)$. It is obvious that

$$M(p-1) \geq \sqrt{p-1}, \qquad M(a) \leq p-1.$$

Is there a better upper bound for $M(a)$?

Write

$$A_n = \begin{cases} 1, & \text{if } mn \equiv a \pmod{p} \text{ has solution } 1 \leq m \leq M, \\ 0, & \text{otherwise.} \end{cases}$$

By a standard technique, we get

$$\begin{aligned} \Big| \sum_{0<n\leq M} A_n - \frac{M^2}{p} \Big| &\leq \log p \max_{1\leq k<p} \Big| \sum_{n=1}^{p} \sum_{\substack{m=1 \\ mn\equiv a \pmod{p}}}^{M} e\Big(\frac{kn}{p}\Big) \Big| \\ &= \log p \max_{1\leq k<p} \Big| \sum_{m=1}^{M} e\Big(\frac{ka\bar{m}}{p}\Big) \Big| \\ &< 4(\log p)^2 p^{\frac{1}{2}}. \end{aligned}$$

The sum

$$\sum_{0<n\leq M} A_n$$

is the number of solutions of the equation

$$mn \equiv a \pmod{p}, \qquad 1 \leq m,\ n \leq M.$$

Hence, if

$$\frac{M^2}{p} \geq 4(\log p)^2 p^{\frac{1}{2}},$$

then the above equation must has a solution, which means

$$M(a) \leq 2(\log p)p^{\frac{3}{4}}.$$

The improvement on the exponent $\frac{3}{4}$ is an open problem.

3) Let $d(n)$ be divisor function. We consider the behaviour of the sum

$$\sum_{n\leq x} d(n)d(n+1).$$

This sum counts the number of integer arrays $(a,\ b,\ r,\ s)$ which satisfy

$$ab \leq x, \qquad ab+1 = rs.$$

We can get the condition

$$ab \equiv -1 \,(\mathrm{mod}\, r).$$

For the fixed r, we calculate how many $a,\ b$. A similar problem with the above one appears, which is on $M(-1)$. By the similar discussion, we get an asymptotic formula

$$\sum_{n\leq x} d(n)d(n+1) = xQ(\log x) + O(x^{\frac{5}{6}+\varepsilon}),$$

where ε a sufficient small positive constant, Q is some quadratic polynomial. For any positive integer a, the sum $\sum_{n\leq x} d(n)d(n+a)$ can be dealt with in the same way. These sums are interested since they appear in the Riemann zeta function theory.

We see the integral

$$\int_0^T |\zeta(\frac{1}{2}+it)|^4 dt.$$

Write $|\zeta|^4 = \zeta^2\overline{\zeta^2}$. Expand this product to produce a double sum the near diagonal terms contain $d(n)d(n+a)$. Then the problem is changed into that for $\sum_{n\leq x} d(n)d(n+a)$. Heath-Brown proved that

$$\int_0^T |\zeta(\frac{1}{2}+it)|^4 dt = TF(\log T) + O(T^{\frac{7}{8}+\varepsilon}),$$

where F is some fourth power polynomial. Motohashi improved the exponent $\frac{7}{8}$ to $\frac{2}{3}$. He used the mean value theory of Kloosterman sums which was developed by Kuznetsov and Iwaniec.

4) Iwaniec made further development on the classic fourth power mean value of ζ function. His object is to estimate the sixth power of ζ function. He proved that

$$\int_0^T |\zeta(\frac{1}{2}+it)|^4 \Big|\sum_{n\leq N}\frac{a(n)}{n^{\frac{1}{2}+it}}\Big|^2 dt \ll T^{1+\varepsilon},$$

where $a(n) = O(1)$, $N \ll T^{\frac{1}{10}}$. He used the estimate for the Kloosterman sum.

Afterwards, Iwaniec and Deshouillers, Watt improved the exponent $\frac{1}{10}$ into $\frac{1}{5}$ and $\frac{1}{4}$. They used the estimate for the Kloosterman sum.

In 2014, Chaohua Jia and A. Sankaranarayanan proved that

$$\sum_{n\leq x} d^2(n) = xP(\log x) + O(x^{\frac{1}{2}}(\log x)^5),$$

where $P(x)$ is some cubic polynomial. We made some refinement on the work of Iwaniec and also used the estimate for the Kloosterman sum.

3 Further development

Let us see the Kloosterman sum with some coefficients. In 1988, D. Hajela, A. Pollington, B. Smith proved that if $(b,\ q) = 1$, then

$$\sum_{\substack{n\leq N\\(n,\ q)=1}} \mu(n)e\Big(\frac{b\bar{n}}{q}\Big) \ll Nq^{\varepsilon}\Big(\frac{(\log N)^{\frac{5}{2}}}{q^{\frac{1}{2}}} + \frac{q^{\frac{3}{10}}(\log N)^{\frac{11}{5}}}{N^{\frac{1}{5}}}\Big).$$

This estimate is non-trivial for $(\log N)^{5+10\varepsilon} \ll q \ll N^{\frac{2}{3}-3\varepsilon}$.

Afterwards, P. Deng, G. Wang and Z. Zeng independently proved that

$$\sum_{\substack{n\leq N\\(n,\,q)=1}}\mu(n)e\Big(\frac{b\bar{n}}{q}\Big)\ll Nq^{\varepsilon}\Big(\frac{(\log N)^{\frac{5}{2}}}{q^{\frac{1}{2}}}+\frac{q^{\frac{1}{5}}(\log N)^{\frac{13}{5}}}{N^{\frac{1}{5}}}\Big).$$

This estimate is non-trivial for $(\log N)^{5+\varepsilon}\ll q\ll N^{1-\varepsilon}$.

P. Deng pointed out that under GRH, one can get

$$\sum_{\substack{n\leq N\\(n,\,q)=1}}\mu(n)e\Big(\frac{b\bar{n}}{q}\Big)\ll q^{\frac{1}{2}}N^{\frac{1}{2}+\varepsilon},$$

which is non-trivial for $q\ll N^{1-4\varepsilon}$. Therefore to break through the limitation $q\leq N$ is the next direction of development.

In 1998, Fouvry and Michel proved that if q is a prime number, $P(x)$ and $Q(x)$ are coprime monic polynomials on $\mathbb{Z}[x]$, $g(x)=\frac{P(x)}{Q(x)}$ is a rational function, then for $N\leq q$, one has

$$\sum_{\substack{p\leq N\\(Q(p),\,q)=1}}e\Big(\frac{g(p)}{q}\Big)\ll q^{\frac{3}{16}+\varepsilon}N^{\frac{25}{32}},$$

where p is the prime number. This estimate is non-trivial for $N\leq q\ll N^{\frac{7}{6}-7\varepsilon}$.

They also proved that for $N\leq q$,

$$\sum_{\substack{n\leq N\\(Q(n),\,q)=1}}\mu(n)e\Big(\frac{g(n)}{q}\Big)\ll q^{\frac{3}{16}+\varepsilon}N^{\frac{25}{32}}.$$

In 2011, Fouvry and Shparlinski proved that for $(b,\,q)=1$, $N^{\frac{3}{4}}\leq q\leq N^{\frac{4}{3}}$, one has

$$\sum_{\substack{N<p\leq 2N\\(p,\,q)=1}}e\Big(\frac{b\bar{p}}{q}\Big)\ll q^{\varepsilon}(q^{\frac{1}{4}}N^{\frac{2}{3}}+N^{\frac{15}{16}}).$$

This estimate is non-trivial for $N^{\frac{3}{4}} \le q \ll N^{\frac{4}{3}-6\varepsilon}$.

They also proved that

$$\sum_{\substack{N<p\le 2N\\(p,\,q)=1}} e\Big(\frac{b\bar{p}}{q}\Big) \ll Nq^{\varepsilon}\Big(\frac{(\log N)^2}{q^{\frac{1}{2}}} + \frac{q^{\frac{1}{4}}(\log N)^{\frac{3}{2}}}{N^{\frac{1}{5}}}\Big).$$

This estimate is non-trivial for $(\log N)^{6+\varepsilon} \ll q \ll N^{\frac{4}{5}-\varepsilon}$.

There are corresponding results for $\mu(n)$.

Naturally one would consider more general situation. When Ke Gong visited Montreal University, Professor Granville suggested him to study the non-trivial estimate for

$$\sum_{\substack{n\le N\\(n,\,q)=1}} f(n)e\Big(\frac{b\bar{n}}{q}\Big)$$

where $f(n)$ is a multiplicative function satisfying $|f(n)| \le 1$.

In the above results, one can apply Vaughan's method in which properties that

$$\sum_{d\,|\,n} \Lambda(d) = \log n$$

or

$$\sum_{d\,|\,n} \mu(d) = \begin{cases} 1, & \text{if } n = 1),\\ 0, & \text{if } n > 1. \end{cases}$$

are used.

But in our situation, we know nothing on $\sum_{d\,|\,n} f(d)$ so that Vaughan's method does not work. We have to seek the new method. Fortunately, we find that the finite version of Vinogradov's inequality which is used by Bourgain, Sarnak and Ziegler is available.

Recently, Ke Gong and Chaohua Jia proved that if $f(n)$ is a multiplicative function, $|f(n)| \le 1$, $q \le N^2$, $(b,\,q) = 1$, then

$$\sum_{\substack{n\le N\\(n,\,q)=1}} f(n)e\Big(\frac{b\bar{n}}{q}\Big) \ll \sqrt{\frac{d(q)}{q}}N(\log\log 6N) + q^{\frac{1}{4}+\frac{\varepsilon}{2}}N^{\frac{1}{2}}(\log 6N)^{\frac{1}{2}} + \frac{N}{\sqrt{\log\log 6N}}.$$

This estimate is non-trivial for

$$(\log\log 6N)^{2+\varepsilon} \ll q \ll N^{2-5\varepsilon}.$$

If $f(n) = \mu(n)$, we can get a bigger range of non-trivial estimate than before. But for the sum on prime numbers, our method is not available.

4 Shifted character sum

We have corresponding result on the shifted character sum.

Let q be a prime number, $(a, q) = 1$, χ be a non-principal Dirichlet character modulo q.

Since the 1930s, I. M. Vinogradov had begun the study on character sums over shifted primes

$$\sum_{p \le N} \chi(p + a),$$

and obtained deep results, where p is prime number. His best known result is a nontrivial estimate for the range $N^{\varepsilon} \le q \le N^{\frac{4}{3}-\varepsilon}$, where ε is a sufficiently small positive constant, which lies deeper than the direct consequence of GRH.

Later, Karatsuba widen the range to $N^{\varepsilon} \le q \le N^{2-\varepsilon}$, where Burgess's method was applied.

For the Möbius function $\mu(n)$, one can get same results on sums

$$\sum_{n \le N} \mu(n)\chi(n + a)$$

as that on sums over shifted primes.

Recently, Ke Gong and Chaohua Jia used the finite version of Vinogradov's inequality to prove the following result:

If $f(n)$ is a multiplicative function satisfying $|f(n)| \le 1$, q $(\le N^2)$ is a prime number and $(a, q) = 1$, χ be a non-principal Dirichlet

character modulo q, then we have

$$\sum_{n\leq N} f(n)\chi(n+a) \ll \frac{N}{q^{\frac{1}{4}}}\log\log(6N)+q^{\frac{1}{4}}N^{\frac{1}{2}}\log(6N)+\frac{N}{\sqrt{\log\log(6N)}}.$$

This estimate is non-trivial for

$$(\log\log(6N))^{4+\varepsilon} \ll q \ll \frac{N^2}{(\log(6N))^{4+\varepsilon}}.$$

References

[1] Ke Gong and Chaohua Jia, *Shifted character sums with multiplicative coefficients*, J. Number Theory, **153**(2015), 364-371.

[2] Ke Gong and Chaohua Jia, *Kloosterman sums with multiplicative coefficients*, Science China Mathematics, **59**(2016), no.4, 653-660.

Mohammed Anwar
Dipartimento di Matematica e Fisica
Università degli studi Roma Tre.
Largo S. L. Murialdo, 1
00146, Roma, Italy.
email: anwar@mat.uniroma3.it

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 2, *Number* 1, *March* 2017, *pages* 21-30

Christophe Delaunay

Atypical averages of root numbers of families of elliptic curves

written by Fabio Caldarola

1 Introduction

An *elliptic curve* is a projective algebraic curve of genus one with a rational point. We recall that, if K is a number field and E is an elliptic curve defined over K, the Mordell-Weil theorem asserts that the (abelian) group $E(K)$ of K-rational points of E, is finitely generated; it means that $E(K) \simeq E(K)_{\text{tors}} \times \mathbb{Z}^r$, where the nonnegative integer $r = \text{rk}_K(E)$ is the *rank* of $E(K)$. Néron, in his thesis [8], generalized this theorem to abelian varieties defined over a field K finitely generated over its prime field and, subsequently, there were several other results of this type. Non-expert readers can find many texts and general references on the theory: we recommend, among others, [11] and [6].
In this paper we consider families of elliptic curves given by an equation of the kind

$$\mathcal{F} : \quad y^2 = x^3 + a_2(t)x^2 + a_4(t)x + a_6(t), \tag{1}$$

where $a_i(t) \in \mathbb{Z}[t]$. In fact, for all but finitely many $t \in \mathbb{Z}$, the specialization $\mathcal{F}(t)$ of $\mathcal{F}$ is an elliptic curve over $\mathbb{Q}$ whose rank is denoted by $r(t)$. Moreover, we recall that the *global root number*

$\varepsilon(t) = \pm 1$ of $\mathcal{F}(t)$ is the sign of the functional equation for the L-series attached to $\mathcal{F}(t)$ (see, for example, [11, App. C.16] or [6, Chap. 16 §3]), and the Birch and Swinnerton-Dyer Conjecture implies $(-1)^{r(t)} = \varepsilon(t)$ (also called the *parity conjecture*; for a nice survey on the subject and for the relations with the Tate-Shafarevich group, see [4]).
We can also view (1) as a single elliptic curve over the rational function field $\mathbb{Q}(t)$: we denote its rank $\mathrm{rk}_{\mathbb{Q}(t)}(\mathcal{F})$ simply by r.
We define the *average root number* of the family (1) over $\mathbb{Z}$, as the following limit (if it exists)

$$\mathrm{Av}(\mathcal{F}) = \lim_{X\to\infty} \frac{1}{2X} \sum_{|t|<X} \varepsilon(t), \tag{2}$$

(where we have set $\varepsilon(t) := 0$ if $\mathcal{F}(t)$ is not an elliptic curve) and it is known that the average root number is zero and the average of $r(t)$ is r or $r+1$, for a large class of families of elliptic curves (see for example [5]); we are instead more interested to find families $\mathcal{F}$ such that $\mathrm{Av}(\mathcal{F}) \neq 0$ and $\mathrm{Av}(\mathcal{F}) \neq (-1)^r$, as better explained in Definition 1.1. Several problems are related with this issue: e.g., for the distribution of zeros of the L-functions $L(s, \mathcal{F}(t))$ and the underlying "symmetry type" of the family $\mathcal{F}$, see [3] and the references therein.

Definition 1.1 Let $\mathcal{F}$ be a non-isotrivial family of elliptic curves given by (1) with rank r over $\mathbb{Q}(t)$. We say that

(i) $\mathcal{F}$ is *potentially parity-biased* (or briefly *potentially biased*) *over* $\mathbb{Z}$ if there is no place of multiplicative reduction except possibly at ∞;

(ii) $\mathcal{F}$ is *parity-biased over* $\mathbb{Z}$ if $\mathrm{Av}(\mathcal{F})$ exists and is non-zero;

(iii) $\mathcal{F}$ has *excess rank over* $\mathbb{Z}$ if $\mathrm{Av}(\mathcal{F})$ exists and $\mathrm{Av}(\mathcal{F}) = -(-1)^r$.

Obviously (iii) implies (ii) and from a conjecture of Helfgott, (ii) would imply (i). In literature there are examples of parity-biased families with $\deg(a_i(t))$ quite large, but these families do not have excess

rank over $\mathbb{Z}$. Hence it is clear that to obtain parity-biased families or with excess rank we need to control the rank r itself, the potentially parity-biased condition and the root numbers $\varepsilon(t)$ with their average.
In this paper we show some results obtained in this sense by S. Bettin, C. David and C. Delaunay; for more details the reader can see the work-in-progress paper [1]. In particular, Theorems 3.1 and 3.2 classify potentially parity-biased families (1) with $\deg a_i(t) \leqslant 2$; then, considering a particular family $\mathcal{F}_a$ given in (5), Theorem 3.3 gives a formula for the root numbers in this family and Theorem 3.4 computes their average $\mathrm{Av}(\mathcal{F}_a)$. In the final part of the paper there are some applications of these results in order to have parity-biased families and families with excess rank.
We close the introductive section with the following well known

Example 1.2 For the Washington's family of elliptic curves, given by

$$\mathcal{F}_1 : \quad y^2 = x^3 + tx^2 - (t+3)x + 1, \tag{3}$$

the rank over $K(t)$ is one for every number field K (see [12, 2]). Moreover, in [9] Rizzo shows that $\varepsilon(t) = -1$ for every $t \in \mathbb{Z}$, and we conclude that this family is parity biased but it does not have excess rank over $\mathbb{Z}$. We notify, finally, that the constant value $\varepsilon(t) = -1\ \forall t \in \mathbb{Z}$ no longer holds out from $\mathbb{Z}$: for instance, $\varepsilon(t) = 1$ for many non integral $t \in \mathbb{Q}$.

2 The rank of a family of elliptic curves

Considering the elliptic curve $\mathcal{F}(t)$ from the family given in (1), we define the *trace of Frobenius* at p of $\mathcal{F}(t)$, denoted by $\mathrm{Tr}_t(p)$, as

$$\mathrm{Tr}_t(p) := \begin{cases} p + 1 - |E(\mathbb{F}_p)| & \text{if } \mathcal{F}(t) \text{ has good reduction at } p, \\ 0 & \text{otherwise}, \end{cases}$$

where $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ and $|E(\mathbb{F}_p)|$ is the number of points in the reduced curve, i.e. the cardinality of $\{(x, y) \in \mathbb{Z}^2 \mid y^2 \equiv x^3 + a_2(t)x^2 + a_4(t)x +$

$a_6(t) \mod p\}$ (see [11, V.2]). Denoting the average value of the trace by

$$A_p(\mathcal{F}) := \frac{1}{p}\sum_{t=0}^{p-1} \mathrm{Tr}_t(p),$$

we can enounce the following

Conjecture 2.1 (Nagao) $\lim_{X\to\infty} \sum_{p\leqslant X} -A_p(\mathcal{F}) \cdot \ln p = \mathrm{rk}_{\mathbb{Q}(t)}(\mathcal{F})$.

In [7] Nagao himself proved the conjecture for five family of elliptic curves, and, as an application of some main results, Rosen and Tate proved in [10] that Nagao Conjecture holds for rational surfaces, hence *a fortiori* when $\deg a_i(t) \leqslant 2$ in (1). Using this fact, for example, we can state the following

Proposition 2.2 *Let $b, e \in \mathbb{Z}$ such that $b^2 - 4e \neq 0$ and consider the following family*

$$\mathcal{F}' : y^2 = x^3 + tx^2 + (-bt - 3b^2 + 9e)x + et + b^3 - 3eb.$$

Then $r \leqslant 1$ and $r = 1$ if and only if $b^2 - 4e$ is $\pm$ a fourth power in $\mathbb{Z} - \{0\}$.

If $b^2 - 4e = 0$ then the curve $\mathcal{F}'(t)$ is singular. To give an idea of the proof we write $x^3+tx^2+(-bt-3b^2+9e)x+et+b^3-3eb$ as $B(x)\cdot t+C(x)$ where $B(x) = x^2 - bx + e$ and $C(x) = x^3 + (-3b^2 + 9e)x + b^3 - 3eb$. Then we have

$$r = \lim_{X\to\infty} \sum_{p\leqslant X} \frac{\ln p}{p} \sum_{x=0}^{p-1}\sum_{t=0}^{p-1} \left(\frac{B(x)t + C(x)}{p}\right), \tag{4}$$

where $\left(\frac{*}{*}\right)$ is the Legendre symbol. In the last sum in (4), the contribution will come from the zeros of B(x) modulo p. It has roots if and only if the discriminant of $B(x)$, i.e. $b^2 - 4e$, is a square modulo p. If $b^2 - 4e$ is not $\pm$ a fourth power, we obtain $r < 1$, so $r = 0$. If $b^2 - 4e$ is $\pm$ a fourth power, we obtain $r = 1$.

3 Potentially biased and parity-biased families

If $\mathcal{F}$ is the family of elliptic curves given by the equation (1) with $\deg a_i(t) \leqslant 2$, to be "potentially parity-biased" is equivalent to the condition

$$(\Delta(t) = 0) \Rightarrow (c_4(t) = 0),$$

where $\Delta(t)$ and $c_4(t)$ have the usual meaning for $\mathcal{F}(t)$ (see, for instance, [11, III.1] or [6, 3 §3]).

Theorem 3.1 *Let $\mathcal{F}$ be given by* (1) *a potentially biased family with* $\deg a_2(t) = 1$ *and* $\deg a_4(t), \deg a_6(t) \leq 2$. *Then $r \leqslant 1$ and up to a linear change of coordinates, $\mathcal{F}$ is one of the following*

(i) $\mathcal{F}' : \ y^2 = x^3 + tx^2 + (-at - 3a^2 + 9b)x + bt + a^3 - 3ab$ *with $a, b \in \mathbb{Z}$; in this case, $r = 1$ if and only if $a^2 - 4b$ is $\pm$ a fourth power in $\mathbb{Z}$.*

(ii) $\mathcal{G} : \ y^2 = x^3 + 3dtx^2 + 3d^2stx + d^3st^2$ *with $d, s \in \mathbb{Z}$; in this case, $r = 1$ if and only if $s \cdot d$ is a square in $\mathbb{Z}$ or -2 times a square.*

(iii) $\mathcal{H} : \ y^2 = x^3 + 3dtx^2 + 3d^2stx + d^3s^2t$ *with $d, s \in \mathbb{Z}$; in this case $r = 0$.*

And what does it happen if, in the statement of the previous theorem, we assume $\deg a_2(t) = 2$? In this case write $a_2(t) = ut^2 + vt + w$, where $u, v, w \in \mathbb{Z}$.

Theorem 3.2 *With such assumptions, up to a linear change of coordinates, $\mathcal{F}$ will be one of the following families*

(i) $\mathcal{F}'(ut^2 + vt + w)$, *and in this case $r \leqslant 3$.*

(ii) $\mathcal{H}(ut^2 + vt + w)$.

(iii) $y^2 = x^3 + 2vt(-4t + 1)x^2 + 4v^2t(2t + 1)x - v^3(4t^2 + 3t + 1)$; *in this case $r \leqslant 1$ and $r = 1$ if and only if v is -2 times a square.*

Now consider the equation of the family $\mathcal{F}'$ in Theorem 3.1 (i) with $b = 0$; more precisely, if $a^2 - 4b$ is a square, there exists a change of variables which transforms $\mathcal{F}'$ in the following

$$\mathcal{F}_a : \; y^2 = x^3 + tx^2 - a(3a + t)x + a^3 \tag{5}$$

(where $a \in \mathbb{Z}$ is not the same as before). For example, note that if we pose $f_a(t) := t^2 + 3at + 9a^2$, we easily find for $\mathcal{F}_a(t)$

$$c_4(t) = 16\, f_a(t), \quad c_6(t) = -32(3a + 2t) f_a(t),$$

$$\Delta(t) = 16a^2 (f_a(t))^2,$$

and, in the special case $a = 1$, we recover the Washington's family $\mathcal{F}_1$ given in (3).
As usual, we denote by $v_p(\cdot)$ the p-adic exponential valuation and by $(\cdot, \cdot)$ the gcd of two integers. Moreover, if $M \in \mathbb{Z}$, let M_0 be the odd part of M, i.e. $M = 2^{v_2(M)} M_0$.

Theorem 3.3 *Let $\varepsilon_a(t)$ be the root number of $\mathcal{F}_a(t)$, then*

$$\varepsilon_a(t) = \; - s_a(t)\, (a_0, t) \cdot \prod_{p \left| \frac{a_0}{(a_0, t)} \right.} (-1)^{1 + v_p(t)} \left(\frac{p^{-v_p(t)} t}{p} \right)^{1 + v_p(t)} \mod 4,$$

where $s_a(t) \in \{-1, 1\}$ is explicit and depends only on a_0 mod 8*, $v_2(a)$* mod 2*, t_0 or $2^{v_2(a)} t$* mod 8.

If q, a are two integers such that $q | a$, we define $\mathrm{Av}_2(q, a)$ as the average of $s_a(qt)$ when t varies with $(t, q) = 1$. Then, using Theorem 3.3, we get

Theorem 3.4 *The following formula holds*

$$\mathrm{Av}(\mathcal{F}_a) = -\frac{1}{|a|} \sum_{\substack{q \,|\, |a| \\ p \left| \frac{a_0}{q_0} \right. \Rightarrow v_p(q) \text{ odd}}} \varphi(|a/q|)\, \chi_4(q_0)\, \mathrm{Av}_2(a, q),$$

where $\chi_4(q_0) \in \{-1, 1\}$ *is congruent to* $q_0 \bmod 4$ *and* $\mathrm{Av}_2(a, q) \in \{0, 1/2, 1\}$.

Note that, in particular, if a is square-free, then $q = a$ is the only divisor appearing in the previous sum, hence

$$\mathrm{Av}(\mathcal{F}_a) = \begin{cases} \pm 1/a & \text{if } a \equiv \mp 1 \mod 8 \\ \pm 1/(2a) & \text{if } a \equiv \pm 3 \mod 8 \\ 0 & \text{if } a \equiv \pm 2 \mod 8 \end{cases}.$$

The first consequence of Theorem 3.4 is the following corollary which gives necessary and sufficient conditions for the family $\mathcal{F}_a$ to be parity-biased.

Corollary 3.5 *The family* $\mathcal{F}_a$ *is parity-biased if and only if* $v_2(a) \neq 1$.

4 Families with excess rank

In this section we preserve the above notations and we continue the study to give some results and examples of families with excess rank. First of all, from Theorem 3.3, if $(a, b) = 1$ we have

$$e_a(at + b) = -\prod_{p \mid a} -\left(\frac{b}{p}\right),$$

and this means that

- if $p \equiv \pm 1 \bmod 8$ and b is not a square mod p, then $\mathcal{F}_p(pt + b)$ has excess rank over Z, with $r = 0$;
- if p is an odd prime and $p \nmid b$, then $\mathcal{F}_{p^2}(pt + b^2)$ has excess rank with $r = 1$.

To obtain families with higher rank we have to consider families of the form $F_{a^2}(ut^2 + vt + w)$: in this case, the rank is $\leqslant 3$.

Definition 4.1 We set

$$\mathcal{H}_{a^2,k}(t) := \mathcal{F}_{a^2}(t^2 - 2at - a^2 + k - a^2(t^2 + u^2)/k).$$

The first thing to do for working with this family, is to write its equation in the form

$$\mathcal{H}_{a^2,k}(t) : \ y^2 = A(x)t^2 + B(x)t + C(x)$$

for suitable polynomials $A(x), B(x), C(x) \in \mathbb{Z}[x]$ (recall (5)). For example, for the first two of them we find

$$A(x) = -\frac{a^2 - k}{k}\, x(x - a^2), \quad B(x) = -2ax(x - a^2).$$

Going further with computations and working on the characteristics of this family, we get results as the following

(a) We can take $k \in \mathbb{Z}$ such that $-\dfrac{a^8}{k}$ and $-\dfrac{ka^8}{(a^2 - k)^3}$ are not squares; in this case $r = 2$.

(b) We can take $k \in \mathbb{Z}$ such that $-\dfrac{a^8}{k}$ or $-\dfrac{ka^8}{(a^2 - k)^3}$ is a square; then $r = 3$.

For example, if we take $a = 2$ and $k = 1$, from (a) we obtain that the family $\mathcal{H}_{4,1}(t)$ has excess rank with $r = 2$. Instead, if we take $p \equiv \pm 1 \mod 8$ and $l \in \mathbb{Z}$ with $p \nmid l$ we find that $\mathcal{H}_{p^2,-p^2}(pt + l)$ has excess rank with $r = 3$.

5 Twist of Washington family

We end the paper going back to the family in the Example 1.2: if $d \in \mathbb{Z} - 0$, the quadratic twist by d of Washington family (3) is

$$E_{d,t} : \ y^2 = x^3 + dtx^2 - (t + 3)d^2x + d^3, \tag{6}$$

which is in fact $\mathcal{F}_d(dt)$ (see (5)).

Theorem 5.1 *For $v_2(d)$ even the following hold*

(i) If $d_0 \equiv \pm 1 \bmod 8$, then $\varepsilon(E_{d,t}) \equiv -|d_0| \bmod 4$.

(ii) If $d_0 \equiv 3 \bmod 8$, then $\varepsilon(E_{d,t}) = \mathrm{sgn}(d_0) \iff t \equiv 0, 1, 2 \bmod 4$.

(iii) If $d_0 \equiv 5 \bmod 8$, then $\varepsilon(E_{d,t}) = \mathrm{sgn}(d_0) \iff t \equiv 1 \bmod 4$.

For $v_2(d)$ odd, $\varepsilon(E_{d,t}) = \mathrm{sgn}(d_0)$ if and only if $t \equiv 0, 3 \bmod 4$.

The rank of $E_{d,t}$ is always zero, unless $d = \pm 1$. If we set $d = d_t(u)$, the generic point of $E_{d_t(u),t}$ is $(ud_t(u), d_t(u)^2)$ and $E_{d_t(u),t}$ has rank $\geqslant 1$ over $\mathbb{Q}(t)$.

Proposition 5.2

(i) If $u \equiv 1 \bmod 4$, then $\varepsilon(E_{d_t(u),t}) = 1$ if and only if $d_t(u) > 0$.

(ii) If $u \equiv 0 \bmod 4$, then $\varepsilon(E_{d_t(u),t}) = 1$ if and only if $d_t(u) < 0$.

References

[1] S. Bettin, C. David and C. Delaunay, *Families of elliptic curves with non-zero average root number*, preprint.

[2] B. Conrad, K. Conrad and H.A. Helfgott, *Root numbers and ranks in positive characteristic*, Adv. in Math. **198** (2005), pp. 684-731.

[3] D. Chantal, D.K. Huynh and J. Parks, *One-level density of families of elliptic curves and the Ratios Conjecture*, J. Res. Number Theory (2015) **1**: 6.

[4] T. Dokchitser, *Notes on the Parity Conjectures*, in *Elliptic Curves, Hilbert Modular Forms and Galois Deformations*, Springer (2013), pp. 201Ű-249.

[5] H.A. Helfgott, *On the behaviour of root numbers in families of elliptic curves*, arXiv:math/0408141 (2009).

[6] D. Husemöller, *Elliptic Curves, 2nd Ed.*, Springer, New York, Graduate Text in Math. **111** (2004).

[7] K.-I. Nagao, $\mathbb{Q}(T)$*-rank of elliptic curves and certain limit coming from the local points*, Manuscr. Math. **92**(1) (1997), pp. 13–32.

[8] A. Néeron, *Problèmes arithmétiques et géométriques rattachés à la notion de rang dŠune courbe algébrique dans un corps*, Bull. Soc. Math. France **80** (1952), pp. 101-Ű166.

[9] O. Rizzo, *Average root numbers for a non-constant family of elliptic curves*, Compositio Math. **136** (2003), pp. 1Ű-23.

[10] M. Rosen and J.H. Silverman, *On the rank of an elliptic surface*, Invent. Math. **133**(1) (1998), pp. 43–67.

[11] J.H. Silverman, *The Arithmetic of Elliptic Curves, 2nd Ed.*, Springer, New York, Graduate Text in Math. **106** (2009).

[12] L. Washington, *Class numbers of the simplest cubic fields*, Math. Comp. **48** (1987), pp. 371Ű-384.

Fabio Caldarola
Dep. of Mathematics and Computer Science
University of Calabria
Cubo 31/B, ponte Bucci
87036 Arcavacata di Rende, Italy.
email: caldarola@mat.unical.it

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 2, *Number* 1, *March* 2017, *pages* 31-36

Alessandro Zaccagnini

Prime numbers in short intervals: the Selberg integral and its generalisations

Written by Federico Campanini

The central problem of Analytic Number Theory is the distribution of prime numbers. The answers to the questions that naturally arise from this problem are only partially known, even assuming powerful and, as yet, unproved hypotheses like Riemann's. Here we are interested in the distribution of prime numbers in "short intervals". With this term we mean intervals of the form $(x, x + y]$, where $y = o(x)$.

Recall the prime-counting function

$$\pi(x) \stackrel{\text{def}}{=} \#\{p \leq x \mid p \text{ is prime}\} \sim \text{li}(x) \stackrel{\text{def}}{=} \int_2^x \frac{dt}{\log t}$$

and the Chebyshev function

$$\psi(x) \stackrel{\text{def}}{=} \sum_{n \leq x} \Lambda(n),$$

where $\Lambda(n)$ is the von Mangoldt function defined to be equal to $\log(p)$ if $n = p^\alpha$ for some p prime and positive integer α, and zero otherwise. It

is well known that the Riemann Hypothesis (RH, for short) is equivalent to either of the two statements

$$\pi(x) = \mathrm{li}(x) + O\left(x^{\frac{1}{2}}\log(x)\right) \quad \text{or} \quad \psi(x) = x + O\left(x^{\frac{1}{2}}(\log x)^2\right).$$

Looking to the "additive" form of the expected main term of both π and ψ, a natural question arises.

Question 1. *For $y \le x$, is it true that*

$$\pi(x+y) - \pi(x) \sim \int_x^{x+y} \frac{dt}{\log t} \quad or \quad \psi(x+y) - \psi(x) \sim y \quad ? \quad (1)$$

In some applications it is sufficient to know that such asymptotic relations hold for most values of y. For measuring precisely what "usually" means, Selberg introduced the variance of the primes in short intervals

$$J(x,\theta) \stackrel{\text{def}}{=} \int_x^{2x} |\psi(t+\theta t) - \psi(t) - \theta t|^2 dt, \quad (2)$$

where $\theta \in [0,1]$ is essentially y/x. On the Riemann Hypothesis we have that

$$J(x,\theta) \ll x^2\theta(\log(2/\theta)^2) \quad \text{uniformly for } x^{-1} \le \theta \le x.$$

It means that in this range of values for θ,

$$\psi(t+\theta t) - \psi(t) = \theta t + O\left((\theta x)^{\frac{1}{2}}\log x\right) \quad \text{for "almost all" } t \in [x, 2x].$$

We now assume RH until the end. As is customary, we denote the generic non-trivial zero of the Riemann ζ-function by $\rho = \frac{1}{2} + i\gamma$. Consider the Montgomery pair-correlation function

$$F(x,T) \stackrel{\text{def}}{=} \sum_{\gamma_1,\gamma_2 \in [0,T]} \frac{4x^{i(\gamma_1-\gamma_2)}}{4+(\gamma_1-\gamma_2)^2}.$$

In [5] Montgomery proved that $F(x,T) \sim \frac{T}{2\pi}\log x$ as $T \to +\infty$ uniformly for $T^{\varepsilon} \leq x \leq T$ and conjectured that $F(x,T) \sim \frac{T}{2\pi}\log T$ as $T \to +\infty$ uniformly for $T \leq x \leq T^{A}$. It means that only the "diagonal" terms (where $\gamma_1 = \gamma_2$) of the sum give a contribution. We are interested in the connection between hypothetical asymptotic formulae for J and F. More precisely, if we write J and F in expansions like

$$J(x,\theta) = \frac{3}{2}x^2\theta(\log(1/\theta) + 1 - \gamma - \log(2\pi)) + R_J(x,\theta)$$

and

$$F(x,T) = \frac{T}{2\pi}\left(\log\frac{T}{2\pi} - 1\right) + R_F(x,T),$$

then we want to answer to the following

Question 2. *Is it possible to compare the size of the error terms $R_J(x,\theta)$ and $R_F(x,T)$ in suitable ranges of uniformity?*

Assuming RH, Montgomery and Soundararajan [6] proved that $R_J(x,\theta) = o(x^2\theta)$ if and only if $R_F(x,T) = o(T)$. In [2], Languasco, Perelli and Zaccagnini studied relations between hypothetical bounds of the type

$$R_J(x,\theta) = O(x^2\theta^{1+\alpha}) \quad \text{and} \quad R_F(x,T) = O(T^{1-\beta}).$$

Their results are as general as they are cumbersome, so, for simplicity, we state a weakened and simplified version of such results, leaving out log-powers and uniformity in the various parameters. Essentially, for $\alpha, \beta > 0$, we have

$$R_J(x,\theta) \ll x^2\theta^{1+\alpha} \qquad \Longrightarrow \qquad R_F(x,T) \ll T^{1-\frac{\alpha}{\alpha+3}},$$
$$R_F(x,T) \ll T^{1-\beta} \qquad \Longrightarrow \qquad R_J(x,\theta) \ll x^2\theta^{1+\frac{\beta}{2}}.$$

We now introduce a new pair-correlation function and connect it to a more general form of the Selberg integral. Let $\tau \in [0,1]$ and define

$$F(x,T,\tau) \stackrel{\text{def}}{=} \sum_{\gamma_1,\gamma_2\in[-T,T]} \frac{4x^{i(\gamma_1-\gamma_2)}}{4+\tau^2(\gamma_1-\gamma_2)^2}.$$

Of course $F(x,T,1)$ is essentially the same as $F(x,T)$. Moreover $F(x^{1/\tau},T,\tau)$ is the pair-correlation function for $Z_\tau(s)=\zeta(s/\tau)$, where Z_τ is (almost) an element of the Selberg Class of degree $\frac{1}{\tau}$ and conductor $\left(\frac{1}{\tau}\right)^{1/\tau}$. Continuing with the properties of $F(x,T,\tau)$, we note that $F(x,T,0)=|\Sigma(x,T)^2|$, where

$$\Sigma(x,T) \stackrel{\text{def}}{=} \sum_{|\gamma|\le T} x^{i\gamma}$$

is the exponential sum that appears in Landau's explicit formula for $\psi(x)$. We also remark that $F(x,T,\tau)$ is difficult to estimate for τ very small (say, $\tau \le 1/T$) because in this case the trivial bound $F(x,T,\tau) \ll \min(T,\tau^{-1})T\log^2 T$ becomes very large.

From now on we assume $\tau > 0$ in order to avoid trivial statements. Let

$$J(x,\tau,\theta) \stackrel{\text{def}}{=} \int_x^{x(1+\tau)} |\psi(t+\theta t)-\psi(\theta)-\theta t|^2 dt$$

Here we are dealing with "short intervals" in two different ways. The obvious conjecture is $J(x,\tau,\theta) \ll x^{2+\varepsilon}\tau\theta$.

There is a conjecture of Gonek involving the behaviour of $\Sigma(x,T)$. It states that $\Sigma(x,T) \ll Tx^{-1/2+\varepsilon} + T^{1/2}x^{\varepsilon}$ for $x,T \ge 2$. This conjecture and an obvious generalisation of Montgomery's "justify us" to work by assuming the following

Assumption (Hypothesis $H(\eta)$)**.** *For some fixed $\eta > 0$ and every $\varepsilon > 0$ we have*

$$F(x,T,\tau) \ll Tx^{\varepsilon} \quad \textit{uniformly for} \quad \begin{cases} x^{\eta} \le T \le x \\ x^{\eta}/T \le \tau \le 1. \end{cases}$$

By using such assuption, in [3], Languasco, Perelli and Zaccagnini proved the following result.

Theorem 1. *If assumption $H(\eta)$ holds for some $\eta \in (0,1)$, then*

$$J(x,\tau,\theta) \ll x^{2+\varepsilon}\tau\theta$$

uniformly for $x^{-1} \le \theta \le x^{-\eta}$ and $\theta x^{\eta} \le \tau \le 1$. Moreover if assumption $H(\eta)$ holds for some $\eta \in (0, 1/2 - 5\varepsilon)$ (for $\varepsilon > 0$ small), then

$$\psi(x+y) - \psi(x) = y + \begin{cases} O(y^{2/3}x^{\eta/3+\varepsilon}) & \text{for } x^{\eta+5\varepsilon} \le y \le x^{1/2} \\ O(y^{1/3}x^{1/6+\eta/3+\varepsilon}) & \text{for } x^{1/2} \le y \le x^{1-\eta}. \end{cases}$$

As an immediate consequence we have

$$\psi(x+y) - \psi(x) = y + O(y^{1/2}x^{\varepsilon})$$

for "almost all" $x \in [x, x(1+\tau)]$ and $y \in [1, x^{1-\eta}]$.

In [4] Languasco, Perelli and Zaccagnini gave an asymptotic result for $F(x,T,\tau)$. Let

$$S(x,\tau) \stackrel{\text{def}}{=} \sum_{n\ge 1} \frac{\Lambda^2(n)}{n} a^2(n,x,\tau)$$

where

$$a(n,x,\tau) \stackrel{\text{def}}{=} \begin{cases} (n/x)^{1/\tau} & \text{if } n \le x \\ (x/n)^{1/\tau} & \text{if } n > x. \end{cases}$$

Then the following Theorem holds.

Theorem 2. *As $x \to +\infty$ we have*

$$F(x,T,\tau) \sim \frac{T}{\pi}\frac{S(x,\tau)}{\tau} + \frac{T\log^2 T}{\pi\tau x^{2/\tau}} + \textit{smaller order terms}$$

uniformly for $\tau \ge 1/T$, provided that $TS(x,\tau) = \infty(\max(x, (\log T)^3/\tau))$.

Of course, this reduces to Montgomery's result for $\tau = 1$. We remark that the Theorem shows the same phenomenon of yielding an asymptotic formula only at "extreme ranges". Notice that if τ is not too

small, say $\tau \geq x^{\varepsilon-1}$, by the Brun-Titchmarsh inequality it follows that $S(x,\tau) \ll \tau \log x$. Moreover, if $y \leq x$ and

$$\psi(x+y) - \psi(x) \sim y \quad \text{uniformly for } y \geq x^{\beta+\varepsilon}$$

then

$$S(x,\tau) \sim \tau \log x \quad \text{uniformly for } \tau \geq x^{\beta+\varepsilon-1}.$$

However, S is erratic for $\tau \leq 1/x$. Essentially, it reduces to the single term given by the prime power closest to x.

Finally, in [4], Languasco, Perelli and Zaccagnini also gave the following asymptotic result.

Theorem 3. *Assume the "Generalized Montgomery Conjecture". Then*

$$J(x,\tau,\theta) \sim \left(1 + \frac{\tau}{2}\right) \tau\theta \log(1/\theta)$$

uniformly for $1/x \leq \theta \leq x^{-\varepsilon}$ *and* $\theta^{1/2-\varepsilon} \leq \tau \leq 1$.

Of course, the first factor here is relevant only if $\tau \gg 1$, when Theorem 3 is a consequence of earlier results. The proof requires a suitable, stronger version of the technique introduced by Goldson and Montgomery in [1], with particular care for the τ-uniformity aspect.

References

[1] D. A. Goldston and H. L. Montgomery, *Pair correlation of zeros and primes in short intervals*, Analytic Number Theory and Diophantine Problems (Boston) (A.C. Adolphson et al., ed.), BirkhÃďuser, 1987, pp. 183–203.

[2] A. Languasco, A. Perelli, and A. Zaccagnini, *Explicit relations between pair correlation of zeros and primes in short intervals*, J. Math. Anal. Appl. **394** (2012), 761–771.

[3] A. Languasco, A. Perelli, and A. Zaccagnini, *An extension of the pair-correlation conjecture and applications*, Math. Res. Lett. **23** (2016), no. 1, 201–220.

[4] A. Languasco, A. Perelli, and A. Zaccagnini, *An extended pair-correlation conjecture and primes in short intervals*, to appear in Trans. Amer. Math. Soc.

[5] H. L. Montgomery, *The pair correlation of zeros of the zeta function*, Analytic number theory (Proc. Sympos. Pure Math., Vol. XXIV, St. Louis Univ., St. Louis, Mo., 1972), Amer. Math. Soc., Providence, R.I., 1973, pp. 181–193.

[6] H. L. Montgomery and K. Soundararajan, *Beyond pair correlation*, Paul ErdÅŚs and his mathematics, I (Budapest, 1999), Bolyai Soc. Math. Stud., vol. 11, JÃąnos Bolyai Math. Soc., 2002, pp. 507–514.

Federico Campanini
Department of Mathematics "Tullio Levi-Civita"
Università degli studi di Padova
Via Trieste, 63
35121-I Padova, Italy.
email: federico.campanini@math.unipd.it

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 2, *Number* 1, *March* 2017, *pages* 39-44

Christian Maire

Decomposition in infinite extensions of number fields

Written by Pierfrancesco Carlucci

1 Introduction

Let p be a prime, $\mathbf{K}$ a number field, and let $\mathbf{K}_\infty/\mathbf{K}$ be a $\mathbb{Z}_p$-extension. Iwasawa showed (cfr. [6]) that the size of the μ-invariant is related to the rate of growth of p-ranks of p-class groups in the tower

$$\mathbf{K} \subset \mathbf{K}_1 \subset \mathbf{K}_2 \subset ... \subset \mathbf{K}_\infty.$$

He showed in 1958 that the vanishing of the μ-invariant for cyclotomic $\mathbb{Z}_p$-extensions of the rationals is equivalent to certain congruences between Bernoulli numbers and he conjectured that $\mu = 0$ for these extensions. This was verified in 1979 for base fields $\mathbf{K}$ which are abelian over $\mathbb{Q}$ by Ferrero and Washington (cfr. [1]) but it remains an unresolved problem for more general base fields. Iwasawa initially conjectured that his μ-invariant vanishes for all $\mathbb{Z}_p$-extensions, but later, in 1973, he was the first to construct $\mathbb{Z}_p$-extensions with arbitrarily large $\mu-$invariants (cfr. [3]).

As a natural development of this branch of algebraic number theory, Maire's work investigates about the other p-adic Galois groups enjoying the aforesaid property (cfr. [4]).

2 The classical case

Let us start by recalling the main costructions in the simplest case, see [3] or [6]. For $n \geq 1$, let $\mathbf{K}_n = \mathbb{Q}(\zeta_{p^n})$ where ζ_{p^n} is a primitive $p^n - th$ root of unity. As customary we set

$$\mathbf{K}_\infty = \bigcup_{n=1}^{\infty} \mathbf{K}_n.$$

Now Gal $(\mathbf{K}_\infty/\mathbb{Q})$ is isomorphic to $\mathbb{Z}_p^\times$ and $\mathbb{Z}_p^\times$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^\times \times \mathbb{Z}_p$. Therefore the fixed field of $(\mathbb{Z}/p\mathbb{Z})^\times$ as Galois group (over $\mathbb{Q}$) isomorphic to $\mathbb{Z}_p$. We call this field $\mathbb{Q}_\infty$ The extension $\mathbb{Q}_\infty/\mathbb{Q}$ is an archetype for $\mathbb{Z}_p$-extensions, i.e. extensions whose Galois group is isomorphich to $\mathbb{Z}_p$. As shown in [6, Chapter 7] one can find a chain of subfields of $\mathbb{Q}_\infty$:

$$\mathbb{Q} = \mathbf{F}_0 \subset \mathbf{F}_1 \subset \cdots \subset \bigcup_{n \geq 0} \mathbf{F}_n = \mathbb{Q}_\infty$$

with

$$\text{Gal}\,(\mathbf{F}_n/\mathbb{Q}) \simeq \mathbb{Z}/p^n\mathbb{Z}.$$

Iwasawa's theorem can then be stated as follows:

Theorem (Iwasawa). *Let $\mathbb{Q}_\infty$ and $\mathbf{F}_n$ be as above. Let p^{e_n} be the exact power of p dividing the class number of $\mathbf{F}_n$. Then there exist integers $\lambda \geq 0, \mu \geq 0$, and ν, all independent of n, and an integer n_0 such that*

$$e_n = \lambda n + \mu p^n + \nu$$

for all $n \geq n_0$

Sketch of proof. We give a brief outline of the proof following [6, section 13.3]. Let $\Gamma = \text{Gal}\,(\mathbb{Q}_\infty/\mathbb{Q}) \simeq \mathbb{Z}_p$. Denote by $\mathbf{L}_n$ the maximal unramified abelian p-extension of $\mathbf{F}_n$. Note that $\mathbf{L}_n$ is Galois over $\mathbf{F}_n$ (being maximal). It follows that $X_n \simeq \text{Gal}\,(\mathbf{L}_n/\mathbf{F}_n)$ is isomorphic to

a p-Sylow subgroup of the ideal class group of $\mathbf{F}_n$, which we call A_n. Set

$$\mathbf{L} = \bigcup_{n \geq 0} \mathbf{L}_n \qquad \text{and} \qquad X = \mathrm{Gal}\,(\mathbf{L}/\mathbb{Q}_\infty)\,.$$

Note that $\mathbf{L}$ is also Galois extension of $\mathbb{Q}$, and so we set $G = \mathrm{Gal}\,(\mathbf{L}/\mathbb{Q})$. The idea is to made X into a Γ-module and hence a $\Lambda := \mathbb{Z}_p[[T]]$-module. Then one can show that actually X is finitely generated and Λ-torsion. Hence it can be shown that X sit inside an exact sequence of Λ-modules of the form

$$0 \to A \to X \to \left(\bigoplus_{i=1}^{s} \Lambda/(p^{n_i}) \right) \oplus \left(\bigoplus_{j=1}^{t} \Lambda/(f_j(T))^{m_j} \right) \to B \to 0,$$

where A and B are finite Λ-modules and each f_j is an irreducible polynomial which is also distinguished (i.e. a monic polynomial whose coefficients, except for the leading coefficient, are all divisible by p). It is not difficult to calculate what happen at the n-th level for modules of the form $\Lambda/(p^n)$ and $\Lambda/(f(T))^m$. One then concludes the proof by transfering back the result to X.

3 Uniform pro-p group

Let Γ be an analytic pro-p group: we can think of Γ as a closed subgroup of $\mathrm{GL}_m(\mathbb{Z}_p)$ for a certain integer m. If $p \geq 3$ we say that Γ is powerful if $[\Gamma, \Gamma] \subset \Gamma^p$ ($[\Gamma, \Gamma] \subset \Gamma^4$ in the case $p = 2$). A powerful pro-p group Γ is said uniform if it has no torsion.

The first task is to define $\mathbb{Z}_p[[\Gamma]]$ and this is done by setting $\mathbb{Z}_p[[\Gamma]] := \varprojlim_U \mathbb{Z}_p[[\Gamma/U]]$, where U runs over the open normal subgroups of Γ. Then we set $\Omega := \mathbb{Z}_p[[\Gamma]]/(p)$, and since the rings Ω and $\mathbb{Z}_p[[\Gamma]]$ are local, noetherian and without zero divisor [2] each of them has a fractional skew field. Call $Q(\Omega)$ the fractional skew field of Ω. Now if $\mathcal{X}$ is a finitely generated $\mathbb{Z}_p[[\Gamma]]$-module, we define $\mathrm{rk}_\Omega(\mathcal{X})$ to be the $Q(\Omega)$-dimension of $\mathcal{X} \otimes_\Omega Q(\Omega)$.

Finally we set:

$$\mu(\mathcal{X}) = \sum_{i \geq 0} \mathrm{rk}_\Omega \left(\mathcal{X}[p^{i+1}]/\mathcal{X}[p^i] \right).$$

Let $\mathbf{L}/\mathbf{K}$ be a uniform p-extension: $\mathbf{L}/\mathbf{K}$ is a normal extension whose Galois group $\Gamma := \mathrm{Gal}(\mathbf{L}/\mathbf{K})$ is a uniform pro-p group. We assume furthermore that the set of places of $\mathbf{K}$ that are ramified in $\mathbf{L}/\mathbf{K}$ is finite.

Let $\mathbf{F}/\mathbf{K}$ be a finite subextension of $\mathbf{L}/\mathbf{K}$. We denote by $A(\mathbf{F})$ the p-Sylow subgroup of the class group of $\mathbf{F}$ and put

$$\mathcal{X}_{\mathbf{L}/\mathbf{K}} := \varprojlim_{\mathbf{F}} A(\mathbf{F}),$$

where the limit is taken over all number fields $\mathbf{F}$ in $\mathbf{L}/\mathbf{K}$ with respect the norm map. We have that $\mathcal{X}_{\mathbf{L}/\mathbf{K}}$ is a finitely generated $\mathbb{Z}_p[[\Gamma]]$-module and hence we can associate as above its μ-invariant which is a generalization of the classical μ-invariant introduced by Iwasawa in the particular case $\Gamma = \mathbb{Z}_p$. Set

$$\mu_{\mathbf{L}/\mathbf{K}} := \mu(\mathcal{X}_{\mathbf{L}/\mathbf{K}}).$$

A first interesting result about μ for this module was proven by Perbet in [5]:

Theorem. *For $n >> 0$ one has:*

$$\log |A(\mathbf{K}_n)/p^n| = \mu_{\mathbf{L}/\mathbf{K}} p^{dn} \log p + O(np^{d(n-1)}),$$

where d is the dimension of Γ as an analytic variety.

We will say that a number field $\mathbf{K}$ is called p-rational if the Galois group of the maximal pro-p-extension of $\mathbf{K}$ unramified outside p is pro-p free. The crucial property of p-rational fields is, informally, that in terms of certain maximal p-extensions with restricted ramification, they behave especially well, almost as well as $\mathbb{Q}$.

The main result can be summarized as follows:

Theorem. *Let Γ be a uniform pro-p group having an automorphism τ of order m with fixed-point-free action, where $m \geq 3$ is co-prime to p. Assume $\mathbf{F}_0$ is a totally imaginary number field admitting a cyclic extension $\mathbf{F}/\mathbf{F}_0$ of degree m such that $\mathbf{F}$ is p-rational.*
Then there exists a finite p-extension $\mathbf{K}/\mathbf{F}$ unramified outside p and a Γ-extension $\mathbf{L}/\mathbf{K}$ with the following property: for any given integer μ_0, there exists a cyclic degree p extension $\mathbf{K}'$ over $\mathbf{K}(\zeta_p)$ such that $\mathbf{L}' = \mathbf{L}\mathbf{K}'$ is a Γ-extension of $\mathbf{K}'$ whose μ-invariant verifies:

$$\mu_{\mathbf{L}'/\mathbf{K}'} \geq \mu_0.$$

If p is a regular prime and m is an odd divisor of $p-1$ we can choose $\mathbf{F} = \mathbb{Q}(\zeta_{p^n})$ for any $n \geq 1$.

References

[1] B. Ferrero and L.C. Washington, *The Iwasawa invariant μ_l vanishes for abelian number fields*, Annals of Mathematics. Second Series 109 (1979), no. 2, 377-395.

[2] J.D. Dixon, M.P.F Du Sautoy, A. Mann and D. Segal, *A*nalytic pro-p-groups, Cambridge studies in advances mathematics 61, Cambridge University Press, 1999.

[3] K. Iwasawa, *On the μ-invariants of $\mathbb{Z}_\ell$-extensions*, Number theory, algebraic geometry and commutative algebra, in honor of Yasuo Akizuki, pp. 1-11, Kinokuniya, Tokyo, 1973.

[4] F. Hajir and C. Maire, *Prime decomposition and the Iwasawa μ-invariant*, 2016.

[5] G. Perbet, *S*ur les invariants dÕIwasawa dans les extensions de Lie p-adiques (French) [On Iwasawa invariants in p-adic Lie extensions] Algebra Number Theory 5 (2011), no. 6, 819Ð848.

[6] L.C. Washington, *Introduction to Cyclotomic Fields*, Volume 83 of Graduate Texts in Mathematics, Springer-Verlag, 1982.

Pierfrancesco Carlucci
Roma, Italy.
email: pieffecar@libero.it

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 2, *Number* 1, *March* 2017, *pages* 45-53

Leo Murata

Relations among arithmetical functions, sum of digits functions and paper-folding sequences

written by Comlan Edmond Koudjinan

1 Introduction

In the field of arithmetical function, we sometimes come across an interesting phenomenon, for example, the difference function of "the sum of digits function for Reflected Binary Code (RBC)", $\{S_{RBC}(n) - S_{RBC}(n-1)\}_{n=1}^{\infty}$, coincides with the regular paper-folding sequence. Here we talk about a generalization of this phenomenon and describe about some relations among the sum of digits functions, automatic sequences and some code systems. This is a survey of the papers [2] and [3], and as for the proofs please refer to these references.

2 An example

2.1 Reflected Binary Code (RBC)

We set

- S_{RBC} is the sum of digits function for RBC

- $\Delta(n) \coloneqq S_{RBC}(n) - S_{RBC}(n-1)$, for any positive integer n.

Then

n	Usual Binary Code	RBC	$S_{RBC}(n)$	$\Delta(n)$
0	0	0	0	
1	1	1	1	+1
2	10	11	2	+1
3	11	10	1	−1
4	100	110	2	+1
5	101	111	3	+1
6	110	101	2	−1
7	111	100	1	−1
8	1000	1100	2	+1
9	1001	1101	3	+1
10	1010	1111	4	+1
⋮	⋮	⋮	⋮	⋮

We would like to point out that
⊙ RBC is a permutation of Binary Code (BC).
⊙ RBC is a "Gray Code ": RBC for $n+1$ and RBC for n differ by exactly one digit. Thus

$$\forall n \in \mathbb{N}, |\Delta(n)| = 1$$

2.2 Regular paper-folding sequence

We fold a paper to the same direction (counter-clockwise).Then we get folds "$V-type$" or "$\Lambda-type$" progressively. Mathematically, we start from the simple sequence

$$\mathfrak{b}_0 = \{1, 1, 1, 1, \cdots\}$$

with $b_n = 1, \forall n \in \mathbb{N}$ and then we construct the sequence $\mathcal{P}_{\mathfrak{b}_0}$, which we call the regular paper-folding sequence as follows

$$\mathcal{P}_{\mathfrak{b}_0} = \{\mathbf{1}, \mathbf{1}, -1, \mathbf{1}, 1, -1, -1, \mathbf{1}\}$$

Thus one has

Theorem 1 ([2])**.**

$$\forall n \in \mathbb{N}, \Delta(n) = \mathcal{P}_{\mathfrak{b}_0}(n).$$

More generally, if

$$\mathfrak{b} := \{b_1, b_2, b_3, \cdots\} \text{ with } b_1 = 1 \text{ and } b_i = \pm 1 \text{ for } i \geq 2$$

Then, as before, we get the generalized paper-folding sequence $\mathcal{P}_{\mathfrak{b}}$

$$\mathcal{P}_{\mathfrak{b}} = \{\mathbf{b_1}, \mathbf{b_2}, -b_1, \mathbf{b_3}, b_1, -b_2, -b_2, \mathbf{b_4}, \cdots\}$$

Thus it is natural to ask ourselves

Question 2. *Is there a corresponding code C such that*

$$\{S_C(n) - S_C(n-1)\}_{n=1}^{\infty} = \{\mathcal{P}_{\mathfrak{b}}(n)\}_{n=1}^{\infty} \ ?$$

The answer is given below.

3 Arithmetical function and sum of digits function

Let go back to the RBC and let define the function

$$\begin{aligned} \xi_{RBC} \colon \mathbb{R}_+ &\to \mathbb{N} \cup \{\infty\} \\ x &\mapsto \sum_{0 \leq n \leq x} \chi_4(n) \end{aligned}$$

where χ_4 is the Dirichlet character modulo 4:

$$\chi_4 \colon \mathbb{N} \cup \{\infty\} \to \mathbb{C} \text{ such that } \chi_4(n) = \begin{cases} 0 & \text{if } n \equiv 0, 2 \mod 4 \\ 1 & \text{if } n \equiv 1 \mod 4 \\ -1 & \text{if } n \equiv 3 \mod 4 \end{cases}$$

Then one has ([2])

$$S_{RBC}(n) = \sum_{k=0}^{\infty} \xi_{RBC}\left(\frac{n}{2^k}\right).$$

This expression could be useful in the study of sum of digits functions.

Remark 3. *For the case of BC, setting*

$$f(n) \coloneqq \begin{cases} 0 & \text{if } n = 0 \\ (-1)^{n-1} & \text{if } n \geq 1 \end{cases}$$

And

$$\xi_{BC}(x) \coloneqq \sum_{0 \leq n \leq x} f(n)$$

Then one has ([2])

$$S_{BC}(n) = \sum_{k=0}^{\infty} \xi_{BC}\left(\frac{n}{2^k}\right).$$

From this expression, one can derive the excellent result on the average of S_{BC} due to H. Delange (1975).

In order to answer question 2, let give a structure of RBC

In RBC $\boxed{0110}$ is the "unit" and this unit comes from $\xi_{RBC}(x)$.

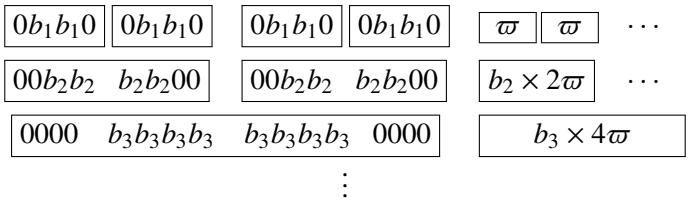
$$\begin{array}{llll} \boxed{0110}\boxed{0110} & \boxed{0110}\boxed{0110} & \boxed{\varpi}\boxed{\varpi} & \cdots \\ \boxed{0011\ \ 1100} & \boxed{0011\ \ 1100} & \boxed{2\varpi} & \cdots \\ \boxed{0000\ \ 1111 \quad 1111\ \ 0000} & & \boxed{4\varpi} & \\ \vdots & & & \end{array}$$

We repeat $\boxed{\varpi}$, $\boxed{2\varpi}$, $\boxed{4\varpi}$,$\cdots$ as above and then, reading vertically, we get the code RBC(n).

Taking into account of the generalization of $\mathfrak{b}_0$ to $\mathfrak{b}$, we can construct by the same way a new code $C_{\mathfrak{b}}$ as follows:
If

$$\mathfrak{b} = \{b_1, b_2, b_3, \cdots\} \text{ with } b_1 = 1 \text{ and } b_i = \pm 1 \text{ for } i \geq 2$$

Then $C_{\mathfrak{b}}$ is (reading vertically)



Thus one can show that $C_{\mathfrak{b}}$ is a Gray code.
Moreover we have:

Theorem 4 ([3])**.**

$$\{S_{C_{\mathfrak{b}}}(n) - S_{C_{\mathfrak{b}}}(n-1)\}_{n=1}^{\infty} = \{\mathcal{P}_{\mathfrak{b}}(n)\}_{n=1}^{\infty}.$$

We remark that $\{\mathcal{P}_{\mathfrak{b}}(n)\}_{n=1}^{\infty}$ is an example of automatic sequences.

4 Some properties of the code $C_{\mathfrak{b}}$

In the case of BC:

$$BC(13) = \underset{(\longrightarrow)}{1011}$$

Which means

$$1 \cdot 2^0 + 0 \cdot 2^1 + 1 \cdot 2^2 + 1 \cdot 2^3 = 13$$

i.e.

$$BC(n) = \underset{(\longrightarrow)}{\beta_1\beta_2\beta_3\cdots}$$

if and only if

$$\sum_{k=1}^{\infty} \beta_k 2^{k-1} = n$$

Moreover, this relation give a bijection between $\{BC(n)\}_{n=1}^{\infty}$ and $\mathbb{N}$.
We can prove a similar result for $C_{\mathfrak{b}}$. For this purpose, let define the function:

$$\mathcal{D}_{\mathfrak{b}} : \mathbb{N} \to \mathbb{Z}$$

Such that if

$$C_{\mathfrak{b}}(n) = \underset{(\longrightarrow)}{\alpha_1\alpha_2\alpha_3\cdots}$$

Then

$$\mathcal{D}_{\mathfrak{b}}(n) \coloneqq \sum_{k=1}^{\infty} \alpha_k 2^{k-1}.$$

Thus we have the following result

Theorem 5 ([3])**.** *Let $K \geq 2$ be an integer.*
If $\mathfrak{b}$ is $K-$periodic then the function $\mathcal{D}_{\mathfrak{b}}$ is a bijection between $\mathbb{N} \cup \{0\}$ and $\mathbb{Z}$.

Remark 6. *If $K = 1$ then $\mathfrak{b} = \mathfrak{b}_0$ and in this case $\mathcal{D}_{\mathfrak{b}_0}$ is a bijection from $\mathbb{N} \cup \{0\}$ onto itself.*

In 2, we remarked that:

$$f(n)=\begin{cases} 0 & \text{if } n = 0 \\ (-1)^{n-1} & \text{if } n \geq 1 \end{cases} \rightsquigarrow \xi_{BC}(x) \rightsquigarrow \sum_{k=0}^{\infty} \xi_{BC}\left(\frac{n}{2^k}\right) = S_{BC}(n)$$

$$\chi_4(n) \rightsquigarrow \xi_{RBC}(x) \rightsquigarrow \sum_{k=0}^{\infty} \xi_{RBC}\left(\frac{n}{2^k}\right) = S_{RBC}(n)$$

Then

Question 7. *What is the arithmetical function $g(n)$ which induces $g(n) \rightsquigarrow \xi_g(x) \rightsquigarrow \sum_{k=0}^{\infty} \xi_g(n/2^k) = S_{C_{\mathfrak{b}}}(n)$?*

To this question, we have the answer which is as follows.
Let $p \geq 2$ and

$\mathcal{A} = \{g : \mathbb{N} \cup \{\infty\} \to \mathbb{C} \text{ with } g(0) = 0\}$ a set of arithmetical functions.

For $g \in \mathcal{A}$, we define the maps

$$\xi_g : \mathbb{R}_+ \to \mathbb{C}, x \mapsto \sum_{0 \leq n \leq x} g(n).$$

And then, we define the maps Φ_p and Ψ_p as follows: $\forall (g,n) \in \mathcal{A} \times \mathbb{N}$,

$$\Phi_p(g)(n) = \sum_{k=0}^{\infty} \xi_g \left(\frac{n}{p^k} \right)$$

$$\Psi_p(g)(n) = \begin{cases} 0 & \text{if } n = 0 \\ g(n) - g(n-1) - \left(g\left(\frac{n}{p}\right) - g\left(\frac{n}{p} - 1\right) \right) & \text{if } n \geq p \text{ and } n \equiv 0 \mod p \\ g(n) - g(n-1) & \text{otherwise} \end{cases}$$

Then we have:

Theorem 8 (Kamiya-Murata [2]). *Φ_p and Ψ_p are bijections from $\mathcal{A}$ onto itself and $\Phi_p^{-1} = \Psi_p$.*

This implies in particular:

$$f \underset{\Psi_2}{\overset{\Phi_2}{\rightleftharpoons}} S_{BC}$$

$$\chi_4 \underset{\Psi_2}{\overset{\Phi_2}{\rightleftharpoons}} S_{RBC}$$

And assuming $\mathfrak{b}$ $K-$periodic then $\exists f_{\mathfrak{b}} \in \mathcal{A}$ such that

$$f_{\mathfrak{b}} \underset{\Psi_{2K}}{\overset{\Phi_{2K}}{\rightleftharpoons}} S_{C_{\mathfrak{b}}}$$

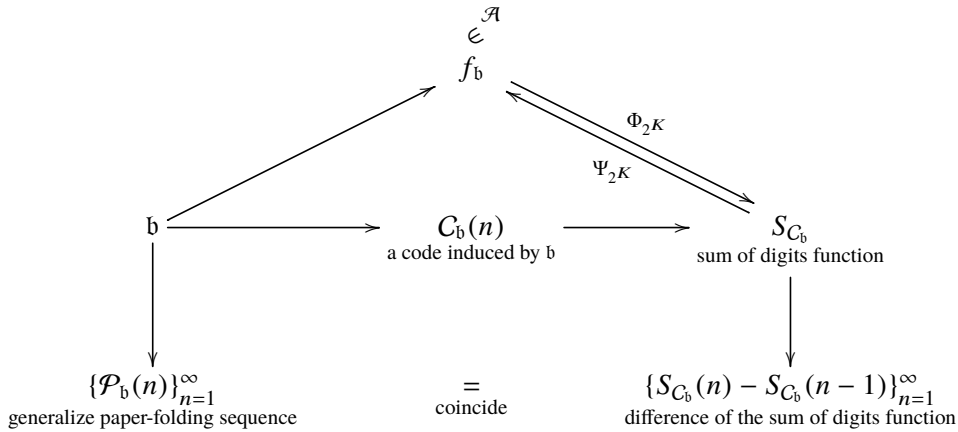
Moreover, we can calculate $f_{\mathfrak{b}}$ as follows:

$$f_{\mathfrak{b}}(n) = \sum_{k=1}^{K} b_k f_0 \left(\frac{n}{2^{k-1}} \right)$$

Where

$$f_0(x) \coloneqq \begin{cases} \chi_4(x) & \text{if } x \in \mathbb{Z} \\ 0 & \text{otherwise} \end{cases}$$

The function $f_{\mathfrak{b}}$ is a $2^{K+1}-$periodic function.
The following diagram summarize this last case:



Theorem 9. *If* $\mathfrak{b}, K, C_{\mathfrak{b}}(n)$ *and* $S_{C_{\mathfrak{b}}}(n)$ *are as above then:*

$$\frac{1}{N}\sum_{n=0}^{N-1} S_{C_{\mathfrak{b}}}(n) = \frac{1}{2\log 2^K}\sum_{k=1}^{K} b_k \log N + F\left(\frac{\log N}{\log 2^K}\right).$$

Where F *is* $1-$*periodic function, continuous, nowhere differentiable. Moreover,* F *admits a Fourier expansion:*

$$F(x) = \sum_{k\in\mathbb{Z}} D_k e^{2\pi i k x}$$

With

$$D_k = \begin{cases} \left(\frac{1}{2} - \frac{1}{\log 2^K}\right) L\left(0, f_{\mathfrak{b}}\right) + \frac{L'\left(0, f_{\mathfrak{b}}\right)}{\log 2^K} & \text{if } k = 0 \\ \dfrac{L\left(\dfrac{2\pi i k}{\log 2^K}, f_{\mathfrak{b}}\right)}{2\pi i k\left(\dfrac{2\pi i k}{\log 2^K} + 1\right)} & \text{if } k \neq 0 \end{cases}$$

Where $L(s, f_{\mathfrak{b}})$ is the Dirichlet series with coefficient $f_{\mathfrak{b}}(n)$.
This is a generalization of Delange's result in [1].

References

[1] H. Delange *Sur la function sommatoire de la function "somme des chiffres"*, L'Enseignement Math., 21, (1975), 31- 47.

[2] Y. Kamiya and L. Murata *Relations among arithmetical functions, automatic sequences, and sum of digits functions induced by certain Gray codes*, Journal de Theorie des Nombres de Bordeaux, 24 (2012), 307-337.

[3] Y. Kamiya and L. Murata *Certain codes related to generalized paperfolding sequences*, Journal de Theorie des Nombres de Bordeaux, 27 (2015), 149-169.

Comlan Edmond Koudjinan
Department of Mathematics
Università degli studi Roma Tre
L.go S. L. Murialdo, n. 1
00146 Roma, Italy.
email: ckoudjinan@mat.uniroma3.it

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 2, *Number* 1, *March* 2017, *pages* 55-60

S. Kanemitsu

Limiting values of Lambert series and the secant zeta-function

written by Lorenzo Menici

The functional equation for the Riemann zeta-function $\zeta(s)$, i.e.

$$\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \pi^{-\frac{1-s}{2}}\Gamma\left(\frac{1-s}{2}\right)\zeta(1-s),$$

can be derived noticing that

$$\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \int_0^\infty x^{\frac{1}{2}s-1}\omega(x)dx,$$

where the function $\omega(x) = \sum_{n=1}^{\infty} e^{-n^2\pi x}$ is trivially related to the theta-function $\theta(x) = \sum_{n=-\infty}^{\infty} e^{-n^2\pi x}$ for which the following theta-transformation formula holds:

$$\theta(x) = \frac{1}{\sqrt{x}}\theta\left(\frac{1}{x}\right).$$

A similar approach can be adapted to obtain the Davenport-Chowla identity [2], [3], [4],

$$\sum_{n=1}^{\infty}\frac{\lambda(n)}{n}\psi(nx) = -\frac{1}{\pi}\sum_{n=1}^{\infty}\frac{\sin 2\pi n^2 x}{n^2}, \tag{1}$$

where $\psi(x) = -\frac{1}{\pi}\sum_{n=1}^{\infty}\frac{\sin 2\pi nx}{n}$ is the saw-tooth Fourier series and $\lambda(n) = (-1)^{\Omega(n)}$ is the Liouville function, whose associated Dirichlet series is

$$\sum_{n=1}^{\infty}\frac{\lambda(n)}{n^s} = \frac{\zeta(2s)}{\zeta(s)}, \qquad \sigma = \Re(s) > 1\,.$$

In (1), on the one hand, there appears $\lambda(n)$ which is a prime number-theoretic entity and, on the other hand, a Riemann's example of a nowhere differentiable function, $\psi(x)$. The integrated identity can be derived from the functional equation only, but to differentiate it one needs the estimate for the error term for the Liouville function which is as deep as the PNT:

$$\sum_{n\le x}\lambda(n) = O(xe^{-c\log^{3/5}x(\log\log x)^{-1/5}})\,.$$

The right-hand side of (1) may be viewed as the imaginary part of the integrated theta-series, so the theta-transformation formula and the functional equation are equivalent. It seems that the uniform convergence of the left-side and the differentiability of the right-side merge as the limiting behavior of a sort of modular function and the Riemann zeta-function, which is modular-function-related.

To establish the Davenport-Chowla identity (1), we need to prove the integrated form by the functional equation and then differentiate. In order to establish an identity in general, we are to integrate it and then differentiate the resulting integral form (or differencing) to deduce it: this is the Abel-Tauber process. It is best known when applied to series. The Riesz sum and its differencing, proving the integrated identity and then differentiating it to obtain the desired identity, the radial integration and radial limits etc. may all be thought of as an Abel-Tauber process. We recall Perron's formula

$$\frac{1}{\Gamma(\varkappa+1)}\sum_{\lambda_k\le x}{}'\,\alpha_k(x-\lambda_n)^{\varkappa} = \frac{1}{2\pi i}\int_c\frac{\Gamma(s)\varphi(s)x^{s+\varkappa}}{\Gamma(s+\varkappa+1)}\,\mathrm{d}s,$$

where the left-hand side sum is called the Riesz sum of order $\varkappa$ and $\varphi(s) = \sum_{k=1}^{\infty} \frac{\alpha_k}{k^s}$, see [6].

Defining $\Theta(z) = \theta(-iz) = \sum_{n=-\infty}^{\infty} e^{\pi i n^2 z}$, the theta-transformation formula now reads

$$\Theta(z) = e^{\frac{\pi i}{4}} z^{-\frac{1}{2}} \Theta\left(-\frac{1}{z}\right) .$$

Then $F(z) = \sum_{n=1}^{\infty} \frac{e^{\pi i n^2 z}}{\pi i n^2}$ is essentially the integral of $\Theta(z)$, since

$$\int_0^z \Theta(z)\, dz = z + 2\left(\sum_{n=1}^{\infty} \frac{e^{\pi i n^2 z}}{\pi i n^2} - \sum_{n=1}^{\infty} \frac{1}{\pi i n^2}\right) = z + 2(F(z) - F(0)) .$$

From [1] we have the following:

Theorem 1.

$$F\left(\frac{2q}{p} + \eth\right) - F\left(\frac{2q}{p} + i\epsilon\right) = S(p,q)\frac{e^{-\pi i/4}}{p}\sqrt{\eth} - \frac{1}{2}h + O(\eth^2)$$

where $S(p,q)$ indicates the quadratic Gauss sum defined for $b \in \mathbb{N}$ by $S(b,a) = \sum_{j=0}^{b-1} e^{2\pi i j^2 \frac{a}{b}}$.

The classical Gauss' quadratic reciprocity law claims whether p is a quadratic residue or non-residue modulo q once q is a quadratic residue or non-residue modulo p is known: but this is not a priori clear. It seems that this is one of the avatars of the symmetry associated with the zeta-functions, i.e. with the functional equation. In our case, we generalize to the following:

Theorem 2.

$$S(p,q) = e^{\frac{\pi}{4}\mathrm{sgn}(q)i}\left(\frac{p}{2|q|}\right)^{1/2} S(4|q|, -\mathrm{sgn}(q)p) .$$

Corollary 1.

$$F\left(\frac{q}{p}+\mathfrak{z}\right)-F\left(\frac{q}{p}+i\epsilon\right)=R(p,q)\frac{e^{-\pi i/4}}{p}\sqrt{\mathfrak{z}}-\frac{1}{2}h+O(\mathfrak{z}^2)\,,$$

where

$$\begin{aligned}
&R(p,2q)=S(p,q)=\varepsilon(p)\left(\frac{q}{p}\right)\sqrt{p}\,,\\
&R(2p,q)=S(4p,q)=e^{\frac{\pi}{4}i}\sqrt{2p}\left(\frac{-p}{q}\right),\\
&R(2B+1,2A+1)=0\,.
\end{aligned}$$

There are many generalizations of the Dedekind eta-function as a Lambert series. Lerch [8] in 1904 introduced the cotangent zeta-function for algebraic irrational z and odd positive integers s as

$$\xi(z,s)=\sum_{n=1}^{\infty}\frac{\cot(n\pi z)}{n^s}\,.$$

Recently, Lalín et al. [7] considered the secant zeta function

$$\psi(z,s)=\sum_{n=1}^{\infty}\frac{\sec(n\pi z)}{n^s}$$

and found its special values at some particular quadratic irrational arguments. The main result of Lalín et al [7, Theorem 3] concerns the difference

$$\begin{aligned}
&(\alpha+1)^{l-1}\psi\left(\frac{\alpha}{\alpha+1},l\right)-(-\alpha+1)^{l-1}\psi\left(\frac{\alpha}{-\alpha+1},l\right)\\
=&\frac{(\pi i)^l}{l!}\sum_{m=0}^{l}(2^{m-1}-1)B_mE_{l-m}\binom{l}{m}\left[(1+\alpha)^{m-1}-(1-\alpha)^{m-1}\right]
\end{aligned}\tag{2}$$

which can be expressed in terms of Bernoulli and Euler numbers.

In [5] we generalized those results. Defining

$$A^*\left(\alpha, s, \frac{1}{2}, 0\right) = \frac{1}{2}\sum_{k=1}^{\infty} k^{s-1}\frac{1}{\cos \pi k\alpha} = \frac{1}{2}\psi(\alpha, 1-s)$$

and

$$V_0 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad V_1 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad V_2 = V_0^2 V_1^{-1} = \begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix},$$

consider the difference

$$D^*(V) = D^*\left(V\alpha, s, \left(\frac{1}{2}, 0\right)\right) = A^*\left(V\alpha, s, \left(\frac{1}{2}, 0\right)\right) - A^*\left(\alpha, s, \frac{1}{2}, 0\right)$$

for each V. We have the following:

Theorem 3.

$$\begin{aligned}
&(\alpha+1)^{-s}A^*\left(\frac{\alpha}{\alpha+1}, s, \left(\frac{1}{2}, 0\right)\right) + (\alpha-1)^{-s}A^*\left(\frac{-\alpha}{\alpha-1}, s, \left(\frac{1}{2}, 0\right)\right) \\
&= \frac{(2\pi)^{-s}e\left[-\frac{s}{4}\right]}{\left(1 - e\left[\frac{s}{2}\right]\right)}\int_{I(\lambda,\infty)} t^{s-1}\sum_{m=0}^{\infty} 2^{-m-1}E_m\frac{t^m}{m!}\sum_{n=0}^{\infty}(2^{1-n}-1)B_n \\
&\times \frac{\{(\alpha+1)^{n-1} + (\alpha-1)^{n-1}\}t^{n-1}}{n!}\,dt\,.
\end{aligned}$$

This Theorem involves the sum of $D^*(V_1)$ and $D^*(V_2)$, which is the genesis of the transformation formula of Lalin et al. [7, Theorem 3], (2), for the secant zeta function. Differently from (2), the result is to be the sum rather than the difference. The oddness of the integer $l-1$ gives a disguised form to the formula. As can be seen in the proof given in the paper [5], $2A^*\left(\alpha, s, \frac{1}{2}, 0\right)$ on the left side and the sum of secant zeta-functions on the right naturally cancel each other. Since this occurs only in such a pairing, this elucidates the hidden structure of the paired transformation formula from a more general standpoint.

References

[1] K. Chakraborty, S. Kanemitsu and H. L. Li, *The quadratic reciprocity and Riemann's non-differentiable function*, Res. Number Theory 1:14 DOI 10.1007/s40993-015-5 (2015), 8 pages.

[2] S. Chowla, *On some infinite series involving arithmetic functions*, Proc. Indian Acad. Sci. A Vol 5 (1937), pp. 511-513.

[3] H. Davenport, *On some infinite series involving arithmetic functions*, Quart. J. Math. Vol 8 (1937), pp. 1781-1786.

[4] H. Davenport, *On some infinite series involving arithmetic functions*, Quart. J. Math. Vol 8 (1937), pp. 1787-1794.

[5] S. Kanemitsu, T. Kuzumaki and B. Magi, *Limiting values of Lambert series and the secant zeta-function*, to appear.

[6] S. Kanemitsu and H. Tsukada, *Contributions to the theory of zeta-functions—modular relation supremacy*, World Sci., London etc. (2014), 303 pages.

[7] M. Lalín, F. Rodrigue and M. Rogers, *Secant zeta functions*, J. Math. Anal. Appl. Vol 409 no. 1 (2014), pp. 197-204.

[8] M. Lerch, *Sur une série analogue aux fonctions modulaires*, C. R. Acad. Sci. Paris. Vol. 138 (1904), pp. 952-954.

Lorenzo Menici
Department of Mathematics
University of Rome RomaTre
Largo San Leonardo Murialdo
00146 Roma, Italy.
email: lorenzo.menici@gmail.com

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 2, *Number* 1, *March* 2017, *pages* 61-81

Michel Waldschmidt

Continued Fractions: Introduction and Applications

written by Carlo Sanna

The continued fraction expansion of a real number x is a very efficient process for finding the best rational approximations of x. Moreover, continued fractions are a very versatile tool for solving problems related with movements involving two different periods. This situation occurs both in theoretical questions of number theory, complex analysis, dynamical systems... as well as in more practical questions related with calendars, gears, music... We will see some of these applications.

1 The algorithm of continued fractions

Given a real number x, there exist an unique integer $\lfloor x \rfloor$, called the *integral part* of x, and an unique real $\{x\} \in [0, 1[$, called the *fractional part* of x, such that

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

If x is not an integer, then $\{x\} \neq 0$ and setting $x_1 := 1/\{x\}$ we have

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

Again, if x_1 is not an integer, then $\{x_1\} \neq 0$ and setting $x_2 := 1/\{x_1\}$ we get

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

This process stops if for some i it occurs $\{x_i\} = 0$, otherwise it continues forever. Writing $a_0 := \lfloor x \rfloor$ and $a_i = \lfloor x_i \rfloor$ for $i \geq 1$, we obtain the so-called *continued fraction expansion* of x:

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots}}},$$

which from now on we will write with the more succinct notation

$$x = [a_0, a_1, a_2, a_3, \ldots].$$

The integers $a_0, a_1, \ldots$ are called *partial quotients* of the continued fraction of x, while the rational numbers

$$\frac{p_k}{q_k} := [a_0, a_1, a_2, \ldots, a_k]$$

are called *convergents*. The convergents are the best rational approximations of x in the following sense: If p and $q > 0$ are integers such that

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

then p/q is a convergent of x. Indeed, of any two consecutive convergents p_k/q_k and p_{k+1}/q_{k+1} of x, one at least satisfies (1) (see [7, Theorems 183 and 184]).

If $x = a/b$ is a rational number, then the method for obtaining the continued fraction of x is nothing else than the Euclidean algorithm for

computing the greatest common divisor of a and b:

$$\begin{aligned} a &= a_0 b + r_0, & 0 \le r_0 < b, \quad & x_1 = b/r_0, \\ b &= a_1 r_0 + r_1, & 0 \le r_1 < r_0, \quad & x_2 = r_0/r_1, \\ r_0 &= a_2 r_1 + r_2, & 0 \le r_2 < r_1, \quad & x_3 = r_1/r_2, \\ &\dots \end{aligned}$$

Therefore, on the one hand, since the Euclidean algorithm always stops, the continued fraction of a rational number is always finite. On the other hand, it is obvious that a finite continued fraction represents a rational number. Hence, in conclusion, we have shown that a real number is rational if and only if its continued fraction expansion is finite.

Note that, if $a_k \ge 2$, then

$$[a_0, a_1, a_2, \dots, a_k] = [a_0, a_1, a_2, \dots, a_{k-1}, a_k - 1, 1], \tag{2}$$

Thus a rational number can be expressed as a continued fraction in at least two ways. Indeed, it can be proved [7, Theorem 162] that any rational number can be written as a continued fraction in exactly two ways, which are given by (2).

2 The number of days in a year

Let us see an application of continued fractions to the design of a calendar. How many days are in a year? A good answer is 365. However, the astronomers tell us that the Earth completes its orbit around the Sun in approximately 365.2422 days. The continued fraction of this figure is

$$365.2422 = [365, 4, 7, 1, 3, 4, 1, 1, 1, 2].$$

The second convergent is

$$365.25 = 365 + \frac{1}{4},$$

which means a calendar of 365 days per year but a leap year every 4 years. The forth convergent gives the better approximation

$$365.2424\ldots = [365, 4, 7, 1] = 365 + \frac{8}{33}.$$

The Gregorian calendar, named after Pope Gregorio XIII who introduced it in 1582, is based on a cycle of 400 years: there is one leap year every year which is a multiple of 4 but not of 100 unless it is a multiple of 400. This means that in 400 years one omits 3 leap years, thus there are

$$400 \cdot 365 + 100 - 3 = 146097$$

days. On the other hand, in 400 years the number of days counted with an year of $365 + \frac{8}{33}$ days is

$$400 \cdot \left(365 + \frac{8}{33}\right) = 146096.9696\ldots$$

a very good approximation!

3 Design a planetarium

Christiaan Huygens (1629–1695) among being a mathematician, astronomer, physicist and probabilist, was also a great horologist. He designed more accurate clocks then the ones available at his time. In particular, his invention of the pendulum clock was a breakthrough in timekeeping. Huygens also built a mechanical model of the solar system. He wanted to design the gear ratios in order to produce a proper scaled version of the planetary orbits. He knew that the time required for the planet Saturn to orbit around the Sun is about

$$\frac{77708431}{2640858} = 29.425448\ldots = [29, 2, 2, 1, 5, 1, 4, \ldots].$$

The forth convergent is

$$[29, 2, 2, 1] = \frac{206}{7}.$$

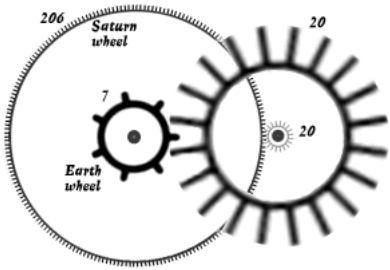


Figure 1: Huygens' planetary gears [1].

Therefore, Huygens made the gear regulating the Saturn's motion with 206 teeth, and the gear regulating Earth's motion with 7 teeth, as shown in Fig. 1.

4 Build a musical scale

The successive harmonics of a note of frequency n are the vibrations with frequencies $2n$, $3n$, $4n$, ... The successive octaves of a note of frequency n are the vibrations with frequencies $2n$, $4n$, $8n$, ... Our ears recognize notes at the octave one from another. Using octaves, one replaces each note by a note with frequency in a given interval, say $[n, 2n[$. The classical choice in Hertz is $[264, 528[$, which means tuning the C tone to 264 Hz (see [6, §20.3]). However, we shall use $[1, 2[$ for simplicity.

Hence, each note with frequency f is replaced by a note with frequency $r \in [1, 2[$ such that

$$f = 2^a r, \quad a = \lfloor \log_2 f \rfloor \in \mathbb{Z}, \quad r = 2^{\{\log_2 f\}} \in [1, 2[.$$

This is a multiplicative version of the Euclidean division.

A note with frequency 3, which is a harmonic of 1, is at the octave of a note of frequency $3/2$. The interval $[1, 3/2[$ is called *fifth*, and the

ratio of its end points is $3/2$. The interval $[3/2, 2[$ is called *fourth*, with ratio $4/3$. The successive fifths are the notes in the interval $[1, 2[$ which are at the octave of notes with frequencies

$$1, 3, 9, 27, 81, \ldots$$

namely:

$$1, \frac{3}{2}, \frac{9}{8}, \frac{27}{16}, \frac{81}{64}, \ldots$$

We shall never come back to the initial value 1, since the Diophantine equation $2^a = 3^b$ has no solution in integers a and b.

In other words, the logarithm of 3 in basis 2 is irrational. Powers of 2 which are close to power of 3 correspond to good rational approximation a/b to $\log_2 3$. Thus it is natural to look at the continued fraction expansion:

$$\log_2 3 = 1.58496250072\ldots = [1, 1, 1, 2, 2, 3, 1, 5, \ldots].$$

The approximation

$$\log_2 3 \approx [1, 1, 1, 2] = \frac{8}{5}$$

means that $2^8 = 256$ is not too far from $3^5 = 243$, that is, 5 fifths produce almost 3 octaves. The next approximation

$$\log_2 3 \approx [1, 1, 1, 2, 2] = \frac{19}{12}$$

tells us that $2^{19} = 524288$ is close to $3^{12} = 531441$, that is

$$\left(\frac{3}{2}\right)^{12} = 129.74\ldots \approx 2^7 = 128.$$

This means that 12 fifths are just a bit more than 7 octaves.

The figure

$$\frac{3^{12}}{2^{19}} = 1.01364,$$

is called the *Pythagorean comma* (or ditonic comma) and produces an error of about 1.36‰, which most people cannot hear.

Further remarkable approximations between perfect powers are:

$$5^3 = 125 \approx 2^7 = 128,$$

that is,

$$\left(\frac{5}{4}\right)^3 = 1.953\ldots \approx 2,$$

so that 3 thirds (ratio 5/4) produce almost 1 octave; and

$$2^{10} = 1024 \approx 10^3,$$

which means that one kibibyte (1024 bytes) is about one kilobyte (1000 bytes), and that doubling the intensity of a sound is close to adding 3 decibels.

5 Exponential Diophantine equations

Another way to avoid the problem that we cannot solve the equation $2^a = 3^b$ in positive integers a and b, might be looking for powers of 2 which are just one unit from powers of 3, that is $|2^a - 3^b| = 1$. This question was asked by the French composer Philippe de Vitry (1291–1361) to the medieval Jewish philosopher and astronomer Levi ben Gershon (1288–1344). Gershon proved that there are only three solutions (a, b) to the Diophantine equation $2^a - 3^b = \pm 1$, namely $(1, 1)$, $(2, 1)$, $(3, 2)$.

Indeed, suppose that $2^a - 3^b = -1$. If $a = 1$ then, obviously, $b = 1$. If $a \geq 2$ then $3^b \equiv 1 \pmod 4$, so that $b = 2k$ for some positive integer k, and consequently

$$2^a = 3^b - 1 = (3^k - 1)(3^k + 1),$$

which implies that both $3^k - 1$ and $3^k + 1$ are powers of 2. But the only powers of 2 which differ by 2 are 2 and 4, hence $k = 1$, $b = 2$, and $a = 3$.

Similarly, suppose that $2^a - 3^b = 1$. Hence $2^a \equiv 1 \pmod 3$, so that $a = 2k$ for some positive integer k and

$$3^b = 2^a - 1 = (2^k - 1)(2^k + 1),$$

which implies that both $2^k - 1$ and $2^k + 1$ are powers of 3. But the only powers of 3 which differ by 2 are 1 and 3, hence $k = 1$, $a = 2$, and $b = 1$.

This kind of questions lead to the study of the so called *exponential Diophantine equations*. A notable case is the *Catalan's equation*

$$x^p - y^q = 1,$$

where x, y, p, q are integers all ≥ 2. In 2002 Mihăilescu [9] showed that $3^2 - 2^3 = 1$ is the only solution, as conjectured by Catalan in 1844.

6 Electric networks

The electrical resistance of a series of two resistances R_1 and R_2 is $R_1 + R_2$ (see Fig. 2). If R_1 and R_2 are instead in a parallel network (see

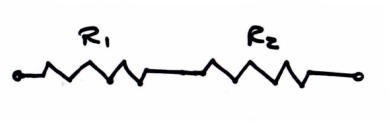


Figure 2: Two resistances R_1 and R_2 in series.

Fig. 3), then the resulting resistance R satisfies

$$\frac{1}{R} = \frac{1}{R_1} + \frac{1}{R_2}.$$

Therefore, it follows easily that the resistance U of the circuit of Fig. 4

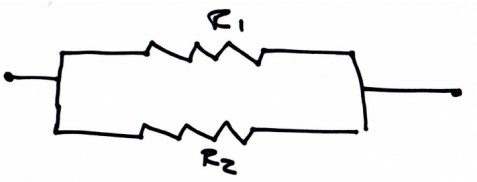


Figure 3: Two resistances R_1 and R_2 in parallel.

is given by

$$U = \cfrac{1}{S + \cfrac{1}{R + \cfrac{1}{T}}}.$$

A similar kind of reasoning shows that the resistance of the infinite

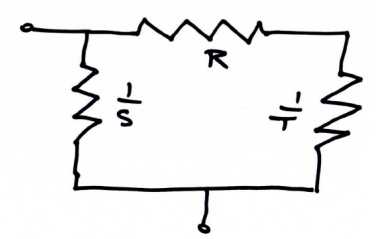


Figure 4: A series–parallel network.

circuit of Fig. 5 is given by the following continued fraction expansion

$$[R_0, S_1, R_1, S_2, R_2, \ldots].$$

Electric networks and continued fractions have been used to solve the "Squaring the square" problem, which states: Is it possible to decompose an integer square into the disjoint union of integer squares, all of which are distinct? The answer to this problem is positive. Indeed, in 1978 Duijvestijn found a decomposition of the 122×122

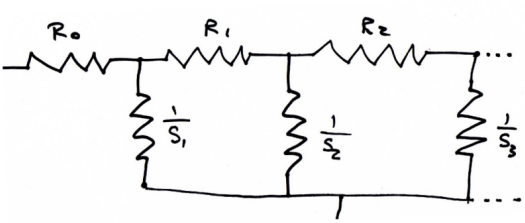


Figure 5: An infinite circuit.

square into 21 distinct integer squares (see Fig. 6). Furthermore, there are no solutions with less than 21 squares, and Duijvestijn's solution is the only with 21 squares (see [3]).

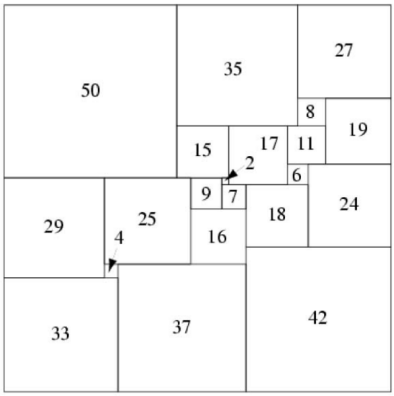


Figure 6: Duijvestijn's solution.

7 Quadratic numbers

Joseph-Louis Lagrange (1736–1813) proved that the continued fraction expansion of a real number x is ultimately periodic, i.e.,

$$x = [a_0, \ldots, a_k, b_1, \ldots, b_h, b_1, \ldots, b_h, \ldots]$$

if and only if x is a quadratic number, that is, x is the root of a quadratic polynomial with rational coefficients (see [5, Chap. IV, §10]).

In such a case, we use the shorter notation

$$x = [a_0, \ldots, a_k, \overline{b_1, \ldots, b_h}],$$

in a ways similar to how it is done for repeating decimals.

7.1 Fibonacci sequence and the Golden Ratio

The Fibonacci sequence $(F_n)_{n\geq 0}$ was introduced by Leonardo Pisano (1170–1250), also known as *Fibonacci*. It is defined as $F_0 := 0$, $F_1 := 1$, and $F_{n+2} = F_{n+1} + F_n$ for all integers $n \geq 0$, and its first terms are

$$0,\ \ 1,\ \ 1,\ \ 2,\ \ 3,\ \ 5,\ \ 8,\ \ 13,\ \ 21,\ \ 34,\ \ 55,\ \ 89,\ \ \ldots$$

The unique positive real numbers Φ satisfying

$$\Phi = 1 + \frac{1}{\Phi} \tag{3}$$

is given by

$$\Phi = \frac{1 + \sqrt{5}}{2}$$

and it is known as the *Golden Ratio*. The Golden Ratio makes its appearance in many different contexts, from Mathematics to Arts [8].

From (3) it is clear that the continued fraction expansion of Φ is

$$\Phi = [1, 1, 1, \ldots] = [\overline{1}],$$

the simplest infinite continued fraction. Notably, the convergents of Φ are precisely the ratios of consecutive Fibonacci numbers

$$[1] = \frac{F_2}{F_1}, \quad [1,1] = \frac{F_3}{F_2}, \quad [1,1,1] = \frac{F_4}{F_3}, \quad [1,1,1,1] = \frac{F_5}{F_4}, \quad \ldots$$

so that

$$\Phi = \lim_{n \to +\infty} \frac{F_{n+1}}{F_n}.$$

7.2 Continued fraction for $\sqrt{2}$

The square root of 2 satisfies

$$\sqrt{2} = 1 + \frac{1}{\sqrt{2} + 1},$$

while

$$\sqrt{2} = 1 + \frac{1}{2 + \dfrac{1}{\sqrt{2} + 1}},$$

hence the continued fraction expansion of $\sqrt{2}$ is given by

$$\sqrt{2} = [1, 2, 2, 2, \ldots] = [1, \overline{2}].$$

7.3 Paper folding

The number $\sqrt{2}$ appears in the A series paper sizes. Precisely, since $\sqrt{2}$ is twice its inverse, i.e., $\sqrt{2} = 2/\sqrt{2}$, folding a rectangular piece of paper with sides in proportion $\sqrt{2}$ yields a new rectangular piece of paper with sides in proportion $\sqrt{2}$ again. The sizes of an A0 paper are defined to be in proportion $\sqrt{2}$ and so that the area is 1 m^2. Thus, rounded to the nearest millimetre, an A0 paper is 841 by 1189 millimetres. Note that

$$\frac{841}{1189} = \frac{29}{49} = [1, 2, 2, 2, 2]$$

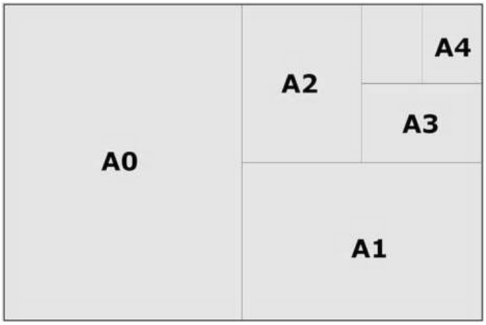


Figure 7: The A series format.

is the fifth convergent of $\sqrt{2}$. The sizes of A1, A2, A3, and so forth are defined by successively halving the A0 paper, as in Fig. 7.

The Golden Ratio Φ has a similar property. If we start with a rectangle with Golden Ratio proportion, then we can fold it in order to get a square and a smaller rectangle which sizes are again in Golden Ratio proportion, as shown in Fig. 8. In fact, the Golden Ratio is the

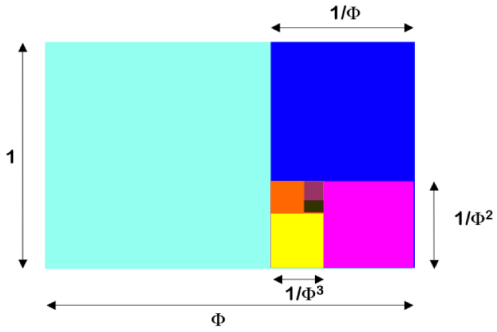


Figure 8: The "Golden rectangle".

unique number with this property.

7.4 The irrationality of $\sqrt{2}$: Two geometric proofs

Considerations similar to the ones of the previous section can lead to "geometric" proofs of the irrationality of $\sqrt{2}$.

A first proof is the following:

- Start with a rectangle having side lengths 1 and $1 + \sqrt{2}$ (see Fig. 9).
- Decompose it into two squares of sides 1 and a rectangle of sides 1 and $1 + \sqrt{2} - 2 = \sqrt{2} - 1$.
- The second rectangle has sides in proportion

$$\frac{1}{\sqrt{2} - 1} = 1 + \sqrt{2},$$

  hence it can be decomposed in two squares and a rectangle whose sides are again in $1 + \sqrt{2}$ proportion.
- This process does not end.

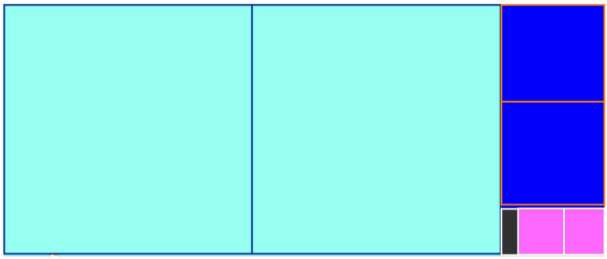


Figure 9: A rectangle dissection proving the irrationality of $\sqrt{2}$.

If we were started with a rectangle having integer side lengths, then it is clear that the process would have stopped after finitely many steps (the side lengths of the successive rectangles produce a decreasing sequence

of positive integers). The same conclusion holds for a rectangle with side lengths in rational proportion (reduce to a common denominator and scale). Therefore, $1 + \sqrt{2}$ is irrational, and so is $\sqrt{2}$.

It is also possible to give a proof in just one dimension:

- Start with an interval of length $t = 1 + \sqrt{2}$ (see Fig. 10).
- Decompose it in two intervals of length 1 and one interval of length $\sqrt{2} - 1 = 1/t$.
- The smaller interval can now be split in two intervals of length $1/t^2$ and one of length $1/t^3$.
- This process does not stop.

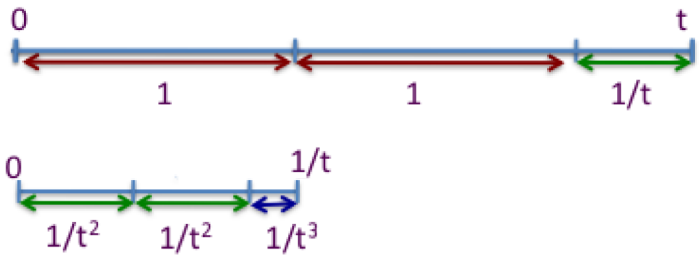


Figure 10: An interval dissection proving the irrationality of $\sqrt{2}$.

Reasoning in a way similar to the previous, it follows easily that if the interval length is a rational number then the process must stop. Thus we get again that $\sqrt{2}$ is irrational.

7.5 The Pell's equation $x^2 - dy^2 = 1$

Let d be a positive integer which is not a square. The Diophantine equation

$$x^2 - dy^2 = 1 \tag{4}$$

is known as *Pell's equation* [5, Chap. IV, §11]. It can be rewritten as

$$\left(x - \sqrt{d}y\right)\left(x + \sqrt{d}y\right) = 1,$$

hence, for $y > 0$, we have that x/y is a rational approximation of $\sqrt{d}$. This is the reason why a strategy for solving (4) is based on the continued fraction expansion of $\sqrt{d}$.

It is quite curious that for relatively small values of d the solutions (x, y) of (4) can be very large. For example, the Indian mathematician Brahmagupta (~628) asked for solution for $d = 92$. The continued fraction expansion of $\sqrt{92}$ is

$$\sqrt{92} = [9, \overline{1, 1, 2, 4, 2, 1, 1, 18}],$$

and a solution $(x, y) = (1151, 120)$ is obtained from

$$[9, 1, 1, 2, 4, 2, 1, 1] = \frac{1151}{120}.$$

Another example is the one of Bhaskara (~1150), that using the same method of Brahmagupta showed that a solution for $d = 61$ is given by

$$x = 1766319049, \quad y = 226153980.$$

But a more impressive example was given by Fermat, who asked to his friend Brouncker a solution for $d = 109$, saying that he choose a small value of d to make the problem not too difficult. However, the smallest solution is

$$x = 158070671986249, \quad y = 15140424455100,$$

which is also given by

$$\left(\frac{261 + 25\sqrt{109}}{2}\right)^6 = 158070671986249 + 15140424455100\sqrt{109}.$$

8 Continued fractions for e and π

Leonard Euler (1707–1784) proved that the continued fraction for e is given by

$$\begin{aligned} e &= [2, 1, 2, 1, 1, 4, 1, 1, 6, 1, \ldots] \\ &= [2, \overline{1, 2m, 1}]_{m \geq 1}. \end{aligned}$$

This result implies that e is not rational neither a quadratic irrational. (Indeed, in 1874 Charles Hermite proved that e is transcendental.) Actually, Euler showed the more general result that for any integer $a \geq 1$ it holds

$$\begin{aligned} e^{1/a} &= [1, a-1, 1, 3a-1, 1, 1, 5a-1, 1, \ldots] \\ &= [\overline{1, (2m+1)a-1, 1}]_{m \geq 1}. \end{aligned}$$

Johann Heinrich Lambert (1728–1777) proved $\tan(v)$ is irrational when $v \neq 0$ is rational. Hence π is irrational, since $\tan(\pi/4) = 1$. The continued fraction expansion of π,

$$\pi = [3, 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 1, 14, 2, 1, 1, \ldots].$$

is much more mysterious than the one of e. Indeed, it is still an open problem to understand if the sequence of partial quotients of π is bounded or not.

9 Continued fractions for analytic functions

Also some analytic functions have a kind of continued fraction expansion. For example, the tangent:

$$\tan(x) = \cfrac{x}{1 - \cfrac{x^2}{3 - \cfrac{x^2}{5 - \cfrac{x^2}{7 - \ddots}}}}.$$

The study of continued fractions of analytic functions is strictly connected to the theory of Padé approximations, which are rational function approximations of analytic functions (see [4]).

10 Gauss map and ergodic theory

Let (X, μ) be a probability space and let $H : X \to X$ be a map that preserve the measure μ, i.e., $\mu(H^{-1}(E)) = \mu(E)$ for any measurable $E \subseteq X$. The Birkhoff's Ergodic Theorem [13, §1.6] states that if H is *ergodic*, which means that $H^{-1}(E) = E$ implies $\mu(E) = 0$ or $\mu(E) = 1$, then for any $f \in L^1_\mu(X)$ we have

$$\lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{n} f(H^{(k)}(x)) = \int_X f \mathrm{d}\mu,$$

for almost all $x \in X$, respect to the measure μ, where $H^{(k)}$ denotes the k-th iterate of H.

We have seen that the partial quotient of a continued fraction are obtained by iterating the map

$$T : x \mapsto \frac{1}{x} - \left\lfloor \frac{1}{x} \right\rfloor,$$

which is called *Gauss map*. It can be proved that the Gauss map preserve the measure

$$\mu(E) := \frac{1}{\log 2} \int_E \frac{\mathrm{d}x}{x+1}, \quad E \subseteq [0, 1],$$

and that it is ergodic. This facts connect continued fractions with the study of chaotic dynamical systems. In particular, exploiting this connection, it can be proved the following result of Aleksandr Yakovlevich Khinchin: For all real numbers

$$x = [a_0, a_1, a_2, \ldots],$$

but a set of Lebesgue measure zero, it holds

$$\lim_{n\to\infty} \sqrt[n]{\prod_{k=1}^{n} a_k} = K_0,$$

where

$$K_0 := \prod_{r=1}^{\infty} \left(1 + \frac{1}{r(r+2)}\right)^{\log_2 r} \approx 2.685452\ldots$$

is known as *Khinchin's constant*.

11 Connection with the Riemann zeta function

We recall that for real $s > 1$, the Riemann zeta function is defined by

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

Notably, $\zeta(s)$ is related to the Gauss map T by the following formula

$$\zeta(s) = \frac{1}{s-1} - s\int_0^1 T(x)x^{s-1}\mathrm{d}s.$$

12 Generalizations of continued expansion in higher dimension

Simultaneous rational approximations of real numbers is a much more difficult problem than the rational approximation of a single number. In fact, the continued fraction expansion algorithm has many specific features and so far there is no extension of this algorithm in higher dimension with all such properties.

However, some attempts has been made, in particular the Jacobi–Perron algorithm [2] uses a kind of ternary continued fraction expansion

to deal with cubic irrationality. This topic is strictly related the *Geometry of numbers*, started by Hermann Minkowski (1864–1909), which is the study of convex bodies and integer vectors in the n-dimensional space $\mathbb{R}^n$. One of the most important result of this field is the LLL algorithm [10], named after Arjen Lenstra, Hendrik Lenstra and Laszlo Lovasz, that given m vectors in $\mathbb{R}^n$ it produces a basis of the lattice they generate with often a smaller norm than the initial ones.

For more recent results see the works of Wolfgang Schmidt, Leonhard Summerer, and Damien Roy [11, 12] in the so-called *Parametric geometry of numbers*.

References

[1] *Chaos in Numberland: The secret life of continued fractions*, http://plus.maths.org/content/chaos-numberland-secret-life-continued-fractions.

[2] L. Bernstein, *The Jacobi-Perron algorithm—Its theory and application*, Lecture Notes in Mathematics, Vol. 207, Springer-Verlag, Berlin-New York, 1971.

[3] C. J. Bouwkamp and A. J. W. Duijvestijn, *Catalogue of simple perfect squared squares of orders* 21 *through* 25, EUT Report-WSK, vol. 92, Eindhoven University of Technology, Department of Mathematics and Computing Science, Eindhoven, 1992.

[4] C. Brezinski, *History of continued fractions and Padé approximants*, Springer Series in Computational Mathematics, vol. 12, Springer-Verlag, Berlin, 1991.

[5] H. Davenport, *The Higher Arithmetic*, eighth ed., Cambridge University Press, Cambridge, 2008, An introduction to the theory of numbers, With editing and additional material by James H. Davenport.

[6] P. U. P. A. Gilbert and W. Haeberli, *Physics in the Arts: Revised edition*, Complementary Science, Elsevier Science, 2011.

[7] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, sixth ed., Oxford University Press, Oxford, 2008, Revised by D. R. Heath-Brown and J. H. Silverman, With a foreword by Andrew Wiles.

[8] H. E. Huntley, *The Divine Proportion: A Study in Mathematical Beauty*, Dover Books on Mathematics, Dover Publications, 1970.

[9] P. Mihăilescu, *Primary cyclotomic units and a proof of Catalan's conjecture*, J. Reine Angew. Math. **572** (2004), 167–195.

[10] P. Q. Nguyen and B. Vallée (eds.), *The LLL algorithm: Survey and applications*, Information Security and Cryptography, Springer-Verlag Berlin Heidelberg, 2010.

[11] D. Roy, *On Schmidt and Summerer parametric geometry of numbers*, Ann. of Math. (2) **182** (2015), no. 2, 739–786.

[12] W. M. Schmidt and L. Summerer, *Diophantine approximation and parametric geometry of numbers*, Monatsh. Math. **169** (2013), no. 1, 51–104.

[13] P. Walters, *An introduction to ergodic theory*, Graduate Texts in Mathematics, vol. 79, Springer-Verlag, New York-Berlin, 1982.

Carlo Sanna
Department of Mathematics "Giuseppe Peano"
Università degli Studi di Torino
Via Carlo Alberto 10
10123 Torino, Italy.
email: carlo.sanna.dev@gmail.com