Proceedings of the 1st mini symposium of the Roman Number Theory Association

Università Europea di Roma

May 7th, 2015

Contents

Prefazione

Il presente volume raccoglie gli interventi presentati nel corso del Primo Simposio dell'Associazione Romana di Teoria dei Numeri. Il convegno, tenutosi nella giornata del 7 Maggio 2015 presso l'Università Europea di Roma, ha rappresentato la prima iniziativa dell'associazione. Come organizzatori del simposio, e promotori della costituenda associazione, ringraziamo gli oratori, per l'alto contributo scientifico offerto, ed agli Scriba che hanno redatto queste note. Ringraziamo anche L'Università Europea di Roma e l'Università Roma Tre per aver finanziato l'evento.

L'associazione Romana di Teoria dei Numeri

L'idea di fondare questa un'associazione nasce dal desiderio di riunire i ricercatori Romani che condividono l'interesse per la Teoria dei Numeri.

Questo primo convegno, di cui sono qui raccolti gli atti, e' una testimonianza del nostro obiettivo di non limitarci ad un programma scientifico specifico ma di fungere un ruolo per la creazione opportunitÃă e servizi per lo sviluppo della Teoria dei Numeri. Tra queste opportunità e servizi rientra il progetto scriba ma anche l'organizzazione di eventi in paesi in via sviluppo e il sostegno ai giovani Teorici dei Numeri sia Europei che da tutto il resto del mondo con una particolare attenzione per quelli dai paesi in via di sviluppo.

L'associazione, che nasce romana e che ha Roma come base, non ha nessuna vocazione campanilista, o nazionale in senso stretto ma aspira ad una visibilità internazionale.

La partecipazione al convegno di numerosi giovani ricercatori, italiani e stranieri

Nell'intento di rendere piu' operativa l'Associazione Romana di Teoria dei Numeri e di realizzare, anche da un punto di vista concreto, i suoi molteplici scopi, abbiamo scelto di trasformarla in una ONLUS.

Il nostro statuto sara' disponibile quanto prima sul sito internet dell'associazione (`www.rnta.eu`) e manifesta chiaramente che i nostri sforzi ed i nostri fondi, saranno consacrati allo sviluppo dello studio della Teoria dei Numeri tramite l'organizzazione diretta di eventi (un convegno annuale a Roma oltre a seminari e conferenze distribuiti nel corso dell'anno), la partecipazione, scientifica e come supporto economico, degli associati ad eventi organizzati in Italia e all'estero sul tema di interesse, ed infine la creazione di un fondo che permetta a giovani teorici dei numeri Italiani ed a matematici provenienti da paesi in via di sviluppo di partecipare alla vita scientifica internazionale nel settore di studio.

1 Il progetto Scriba

Gli atti di un convegno raccolgono di norma i contributi piú significativi presentati durante il convegno stesso. La scelta editoriale operata in questo caso è stata leggermente diversa. Nelle settimane che hanno preceduto il nostro simposio, abbiamo analizzato la lista dei partecipanti ed individuato una rosa di Dottorandi e giovani Post-Doc Italiani e stranieri cui abbiamo proposto di svolgere un compito particolare: quello dello "scriba". Ciascuno degli studiosi cosí individuati è stato poi associato ad uno degli oratori del convegno di cui doveva seguire l'intervento con particolare attenzione e a cui doveva poi rivolgersi per raccogliere tutte le informazioni complementari (note bibliografiche, approfondimenti eccetera) che gli permettessero di essere l'autore di

un articolo dedicato a quella particolare conferenza.

I motivi di questa scelta rimandano a quello che è uno dei temi di predilezione dell'Associazione Romana di Teoria dei Numeri: l'apertura ai piú giovani e la loro sensibilizzazione ai nostri temi di ricerca. Questo lavoro ha infatti consentito ai nostri "scriba" di confrontarsi con il difficile compito di scrivere su un argomento distinto da quello della loro tesi di Dottorato o dei loro primi articoli (spesso ad essa strettamente legati) esplorando un nuovo tema di ricerca scelto fra i filoni attualmente piú promettenti; il beneficio diretto, in termini di ampliamento degli orizzonti ed approfondimento della cultura scientifica, ha persuaso tutti i partecipanti da noi sollecitati ad accettare entusiasticamente. Inoltre, la possibilità di lavorare a stretto contatto con ricercatori di maggiore esperienza ha certamente rappresentato per i nostri "scriba" un ulteriore fattore di crescita personale. I testi sono ovviamente stati sottoposti ai relatori per approvazione e poi ripresi dai curatori del volume.

Marina Monsurrò
Dipartimento di Economia
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

Foreword

This volume contains the proceeding of the first miny symposium of the Roman Number Theory Association. The conference, was held on May 7, 2015 at the Università Europea di Roma, and it represented the first initiative of the association. As organizers of the symposium, and promoters of the constituent association, we 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 founding this association stems from the desire to bring together Roman researchers who share an interest in number theory.

This first conference, whose proceedings are collected here, is evidence of our goal: to be a key player in the development of a strong Roman community of number theorists, and by this we do not only intend to foster a specific scientific program but also, and more importantly, to create a framework of opportunities for scientific cooperation for those interested in number theory. Among these opportunities we can enlist the Scriba project as well as international cooperation with developing countries and the support of young researcher in number theory with special regards to those coming from developing country.

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

In an effort to make the Roman Number Theory Association work efficiently and achieve its multiple goals we chose to turn it into an NGO.

Our statute will be available as soon as possible on the association's website (www.rnta.eu) and it clearly shows 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; participation, 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 itself. The editorial choice made in this case was slightly different. In the weeks leading up to our first symposium, we pondered upon the list of participants and 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 of the chosen young scholar was then paired with one of the speakers and was asked to prepare a written report on the talk of the speakers 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. It has to be said that all the speakers and scriba joined the project enthusiastically.

The reasons for this choice lies in the most essential aim of our Association: introducing young researcher to number theory, in all its possible facets. The benefits of this project were twofold: on one side

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 side they had the possibility to collaborated 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.

Marina Monsurrò
Dipartimento di Economia
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

OFFICIAL PHOTO AND PARTICIPANTS LIST

1. Marina Monsurrò (Università Europea di Roma)
2. Leonardo Zapponi (Université Pierre et Marie Curie)
3. Claudio Stirpe (Sapienza Università di Roma)
4. Pietro Mercuri (Sapienza Università di Roma)
5. Marco Cantarini (Università di Parma)
6. Alina Ostafe (University of New South Wales)
7. Mohammed Anwar (Università Roma Tre)
8. Christian Mauduit (Université d'Aix-Marseille)
9. Valerio Dose (Università di Roma "Tor Vergata")
10. Joël Rivat (Université d'Aix-Marseille)
11. Giulio Meleleo (Università Roma Tre)
12. Lorenzo Menici (Università Roma Tre)
13. Athanasios Angelakis (Universiteit Leiden)
14. Alessandro Zaccagnini (Università di Parma)
15. Valerio Talamanca (Università Roma Tre)
16. Pieter Moree (Max Plank Institute for Mathematics)
17. Flaminio Flamini (Università di Roma "Tor Vergata")
18. Biagio Palumbo (Università Roma Tre)
19. Andreas Bender (Pohang University of Science and Technolog)

20. Nilakantha Paudel (Università Roma Tre)
21. Cihan Pelhivan (Università Roma Tre)
22. Francesco Pappalardi (Università Roma Tre)
23. Andrea Di Lorenzo (Sapienza Università di Roma)
24. Lorenzo Boni (Sapienza Università di Roma)
25. Floriana Amicone (Sapienza Università di Roma)
26. Nathan Jones (University of Illinois at Chicago)
27. Peter Stevenhagen (Universiteit Leiden)

First Minisymposium of the RNTA, May 7, 2015

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 1, *Number* 1, *March* 2016, *pages* 1–5

Pietro Mercuri

New results on the Class Number One problem for Functions Fields

written by Floriana Amicone, Alessandro Boni
and Andrea Di Lorenzo

Let p be a prime number and let q be a power of p. This talk was devoted to the classification of algebraic function fields in one variable over the finite field $\mathbb{F}_q$ with class number one. An immediate consequence of the Riemann-Roch theorem is that every algebraic function field in one variable over $\mathbb{F}_q$ with genus 0 has class number 1. In 1971 Mac Rae classified algebraic function fields in one variable over $\mathbb{F}_q$ with positive genus and class number 1 having rational places. In 1972 Madan and Queen gave a full list of zeta functions of the algebraic function fields in one variable over $\mathbb{F}_q$ with positive genus and class number 1. They also proved that an algebraic function field in one variable over $\mathbb{F}_q$ with genus greater than 4, has class number greater than 1.

The following theorem was the first attempt to give a complete classification:

Theorem 1 (Leitzel, Madan, Queen – 1975) *Let K be an algebraic function field in one variable over $\mathbb{F}_q$ with genus g such that $0 < g < 4$ and class number 1. Then K is isomorphic to the algebraic function field $\mathbb{F}_q(x, y)$ in one variable defined by one of the following equations:*

(i) $y^2 + y + x^3 + x + 1 = 0$, *with* $q = 2$ *and* $g = 1$*;*

(ii) $y^2 + y + x^5 + x^3 + 1 = 0$, *with* $q = g = 2$*;*

(iii) $y^2 + y + (x^3 + x^2 + 1)(x^3 + x + 1)^{-1} = 0$, *with* $q = g = 2$*;*

(iv) $y^4 + xy^3 + (x^2 + x)y^2 + (x^3 + 1)y + x^4 + x + 1 = 0$, *with* $q = 2$ *and* $g = 3$*;*

(v) $y^4 + (x^3 + x + 1)y + x^4 + x + 1 = 0$, *with* $q = 2$ *and* $g = 3$*;*

(vi) $y^2 + 2x^3 + x + 1 = 0$, *with* $q = 3$ *and* $g = 1$*;*

(vii) $y^2 + y - x^3 + \alpha = 0$, *with* $q = 4$, $\alpha \in \mathbb{F}_4^{\times}$ *and* $g = 1$, *where* α *is a generator of the multiplicative group* $\mathbb{F}_4^{\times}$.

In what follows, an algebraic function field in one variable over $\mathbb{F}_2$ with genus 4 and class number 1 is constructed and this leads to a complete classification of the algebraic function fields in one variable over $\mathbb{F}_q$ with class number one.

Definition 1 *An algebraic curve defined over* $\mathbb{F}_q$ *is called a* n-pointless curve *if it has no* $\mathbb{F}_{q^m}$ *rational points for each* $m \leq n$*. Similarly, an algebraic function field in one variable over* $\mathbb{F}_q$ *corresponding to a* n*-pointless curve is called a* n-pointless function field*.*

Every genus 0 algebraic curve defined over $\mathbb{F}_q$ has $\mathbb{F}_q$-rational points (this follows from the Riemann hypothesis for function fields, proved by Weil in 1948). Also, in 1936, Hasse proved that each genus 1 algebraic curve defined over $\mathbb{F}_q$ has $\mathbb{F}_q$-rational points.

In 2013 (cf [8]) Stirpe proved that, for any positive integer n, there exists an algebraic function field in one variable over $\mathbb{F}_q$ without places of degree smaller than n with genus smaller than Cq^n, where $C > 0$ is a suitable constant depending only on the prime p. This construction,

with $n = 3$, gives us the algebraic function field $\mathbb{F}_2(x, y)$ in one variable defined by the following equation:

$$\begin{aligned} & y^5 + y^3 + y^2(x^3 + x^2 + x) + \\ & + y\frac{x^7 + x^5 + x^4 + x^3 + x}{x^4 + x + 1} + \\ & + \frac{x^{13} + x^{12} + x^8 + x^6 + x^2 + x + 1}{(x^4 + x + 1)^2} = 0. \end{aligned}$$

This algebraic function field over $\mathbb{F}_2$ is 3-pointless, has genus 4 and class number 1. From now on, we denote it by L.

Theorem 2 (Mercuri, Stirpe – 2015) *Let K be an algebraic function field in one variable over $\mathbb{F}_2$ with genus 4 and class number 1. Then K is isomorphic to L.*

Using this result, the classification is given in the following way:

Theorem 3 (Leitzel, Madan, Queen; Mercuri, Stirpe et al.) *Let K be an algebraic function field in one variable over $\mathbb{F}_q$ with positive genus and class number 1. Then K is isomorphic to the algebraic function field $\mathbb{F}_q(x, y)$ in one variable defined by one of the following equations:*

(i) $y^2 + y + x^3 + x + 1 = 0$, *with* $q = 2$ *and* $g = 1$;

(ii) $y^2 + y + x^5 + x^3 + 1 = 0$, *with* $q = g = 2$;

(iii) $y^2 + y + (x^3 + x^2 + 1)(x^3 + x + 1)^{-1} = 0$, *with* $q = g = 2$;

(iv) $y^4 + xy^3 + (x^2 + x)y^2 + (x^3 + 1)y + x^4 + x + 1 = 0$, *with* $q = 2$ *and* $g = 3$;

(v) $y^4 + (x^3 + x + 1)y + x^4 + x + 1 = 0$, *with* $q = 2$ *and* $g = 3$;

(vi) $y^2 + 2x^3 + x + 1 = 0$, *with* $q = 3$ *and* $g = 1$;

(vii) $y^2 + y - x^3 + \alpha = 0$, *with* $q = 4$, $\alpha \in \mathbb{F}_4^\times$ *and* $g = 1$, *where* α *is a generator of the multiplicative group* $\mathbb{F}_4^\times$*;*

(viii) $y^5 + y^3 + y^2(x^3 + x^2 + x) + y(x^7 + x^5 + x^4 + x^3 + x)(x^4 + x + 1)^{-1} + (x^{13} + x^{12} + x^8 + x^6 + x^2 + x + 1)(x^4 + x + 1)^{-2} = 0$, *with* $q = 2$ *and* $g = 4$.

At the same time, independently, Shen and Shi and also Rzedowski-Calderòn and Villa-Salvador proved the same result. The proof of Shen and Shi is a correction of the original argument of Leitzel, Madan and Queen, while Rzedowski-Calderòn and Villa-Salvador showed that there exists only one (up to isomorphism) function field with genus 4 and class number 1, without using the example found by Stirpe.

References

[1] H. Hasse, *Zur Theorie der abstrakten elliptischen Funktionkörper I, II, III*, J. Reine Angew. Math., **175** (1936), 55-62, 69-88, 193-208.

[2] J. Leitzel, M. Madan, C. Queen, *Algebraic function fields of class number one*, Journal of Number Theory, **7** (1975), 11-27.

[3] M. Madan, C. Queen, *Algebraic function fields of class number one*, Acta Arithmetica, **20** (1972), 423-432.

[4] R. E. Mac Rae. *On unique factorization in certain rings of algebraic functions*, Journal of Algebra, **17** (1971).

[5] P. Mercuri, C. Stirpe, *Classification of function fields with class number one*, Journal of Number Theory, **154** (2015), 365-374.

[6] M. Rzedowski-Calderòn, G. Villa-Salvador, *Congruence Function Fields with Class Number One*, Arxiv (2014).

[7] Q. Shen, J. Shi, *Function Fields of class number one*, Arxiv (2015).

[8] C. Stirpe, *An upper bound for the minimum genus of a curve without points of small degree*, Acta Arithmetica, **160** (2013), 115-128.

[9] C. Stirpe, *A counterexample to 'Algebraic function fields with small class number'*, Journal of Number Theory, **143** (2014), 402-404.

Floriana Amicone, Alessandro Boni, Andrea Di Lorenzo
Dipartimento di Matematica
Sapienza Università di Roma
Piazzale Aldo Moro 5
00185 Roma, Italy

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 1, *Number* 1, *March* 2016, *pages* 7–15

Peter Stevenhagen

Adelic points of elliptic curves

written by Athanasios Angelakis

1 Introduction

In the first part of his thesis [1], Angelakis studies absolute abelian Galois groups $A_K = \mathrm{Gal}(K^{\mathrm{ab}}/K)$ of number fields K using class field theory. It was already known that for imaginary quadratic number fields K, K' we can have $A_K \cong A_{K'}$, as topological groups, even if K and K' are *not* isomorphic as number fields (Onabe, 1976). Angelakis' striking and very explicit result is the following;

Theorem 1.1 *There exist "many" imaginary quadratic number fields K having*

$$A_K \cong U \stackrel{\mathrm{def}}{=} \widehat{\mathbb{Z}}^2 \times \prod_{m=1}^{\infty} \mathbb{Z}/m\mathbb{Z},$$

as topological groups.

In order to make more precise what "many" means, data can be taken from Watkins' table. For example, the imaginary quadratic number fields K having prime class number lower than 100. From these 2356 number fields, 2291 have absolute abelian Galois group A_K isomorphic to U. Numerically, it seems that an imaginary quadratic number field K of class number p has $A_K \cong U$ with probability $1 - \frac{1}{p}$. This observation leads to:

Conjecture 1.2 *100% of all imaginary quadratic number fields K of prime class number have $A_K \cong U$.*

Not much can be proven here, as distribution results both for the occurrence of prime class numbers and for the average splitting behavior in the analysis of A_K, are lacking. However the same techniques can be applied to a different problem that, although at first sight more complicated, does yield proven theorems.

2 Elliptic curves over K

In class field theory, Galois groups arise as quotients of the multiplicative group $\mathbb{A}_K^*$ of K-ideles. Here the interest lies in the adelic point group $E(\mathbb{A}_K)$ of an elliptic curve E defined over a number field K. The distribution of $E(K)$ as finitely generated abelian group is a very hard problem, even over $\mathbb{Q}$.

Even though $\mathbb{A}_K = \prod_{\mathfrak{p}}' K_{\mathfrak{p}}$ is a *restricted* product of all completions $K_{\mathfrak{p}}$ of K, the adelic point group of an elliptic curve E/K equals

$$E(\mathbb{A}_K) = \prod_{\mathfrak{p}} E(K_{\mathfrak{p}}).$$

For "large" $\mathfrak{p}$ there are many different possibilities for the $\mathfrak{p}$-adic group $E(K_{\mathfrak{p}})$. Still, the product is surprisingly rigid:

Theorem 2.1 *Let K be a number field of degree n. Then for 'almost all' elliptic curves E/K, the adelic point group $E(\mathbb{A}_K)$ is topologically isomorphic to the universal group*

$$\mathcal{E}_n = (\mathbb{R}/\mathbb{Z})^n \times \widehat{\mathbb{Z}}^n \times \prod_{m=1}^{\infty} \mathbb{Z}/m\mathbb{Z}$$

associated to the degree n of K.

Based on the counting of integral Weierstrass models as in [4], the notion of 'almost all' in this theorem is the following one: for elements a and b in the ring of integers O_K of K satisfying $\Delta(a,b) = -16(4a^3 + 27b^2) \neq 0$, we write $E(a,b)$ for the elliptic curve defined by the affine Weierstrass equation $y^2 = x^3 + ax + b$. Now fix a norm $||.||$ on $\mathbb{R} \otimes_{\mathbb{Z}} O_K^2 \cong \mathbb{R}^{2[K:\mathbb{Q}]}$. Then for any positive real number X, the set B_X of elliptic curves $E(a,b)$ with $||(a,b)|| < X$ is finite. We say that *almost all* elliptic curves over K have some property, if the fraction of elliptic curves $E(a,b)$ in B_X having that property tends to 1 when $X \in \mathbb{R}_{>0}$ tends to infinity.

Our notion of 'almost all' still allows for large numbers of elliptic curves E/K to have adelic point groups different from the universal group in Theorem 2.1, as the following theorem states.

Theorem 2.2 *Let K be a number field of degree n. Then there exist infinitely many elliptic curves E/K that are pairwise non-isomorphic over an algebraic closure of K, and for which $E(\mathbb{A}_K)$ is a topological group not isomorphic to $\mathcal{E}_n$.*

The adele ring of K naturally decomposes as a product $\mathbb{A}_K = \mathbb{A}_K^{\infty} \times \mathbb{A}_K^{\mathrm{fin}}$, in which $\mathbb{A}_K^{\infty}$ is the product of the archimedean completions of K, and the *ring of finite K-adeles* $\mathbb{A}_K^{\mathrm{fin}} = \prod_{\mathfrak{p}}' K_{\mathfrak{p}}$ is the restricted product (in the sense explained above) of the non-archimedean completions of K. The adelic point group of an elliptic curve E/K decomposes correspondingly as a product

$$E(\mathbb{A}_K) = E(\mathbb{A}_K^{\infty}) \times E(\mathbb{A}_K^{\mathrm{fin}}). \tag{1}$$

The best strategy is to deal with these factors separately.

3 The Structure of $E(\mathbb{A}_K)$

Every completion of K at an infinite prime $\mathfrak{p}$ of K is isomorphic to either $\mathbb{R}$ or $\mathbb{C}$, depending on whether $\mathfrak{p}$ is real or complex. For $\mathfrak{p}$ complex

and E/K an elliptic curve, $E(K_\mathfrak{p})$ is a topological group isomorphic to $(\mathbb{R}/\mathbb{Z})^2$, by the well-known fact that we have $E(K_\mathfrak{p}) \cong \mathbb{C}/\Lambda$ for some lattice $\Lambda \subset \mathbb{C}$ by the complex analytic theory.

For $\mathfrak{p}$ real and E/K an elliptic curve, there are two possible types of groups $E(K_\mathfrak{p})$, and they may be distinguished by looking at the discriminant Δ_E of the elliptic curve. The *sign* of $\Delta(E)$ is well-defined for every real prime $\mathfrak{p} : K \to \mathbb{R}$ of K, and for such $\mathfrak{p}$ we have

$$E(K_\mathfrak{p}) \cong \begin{cases} \mathbb{R}/\mathbb{Z}, & \text{if } \Delta(E) <_\mathfrak{p} 0; \\ \mathbb{R}/\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, & \text{if } \Delta(E) >_\mathfrak{p} 0. \end{cases} \tag{2}$$

The following is easily proved

Proposition 3.1 *Let K be a number field of degree n, and E/K an elliptic curve with discriminant $\Delta_E \in K^*/(K^*)^{12}$. Then there exists an isomorphism of topological groups*

$$E(\mathbb{A}_K^\infty) \cong (\mathbb{Z}/2\mathbb{Z})^r \times (\mathbb{R}/\mathbb{Z})^n. \tag{3}$$

Here $r \leq n$ is the number of real primes $\mathfrak{p}$ of K for which we have $\Delta(E) >_\mathfrak{p} 0$.

Let $\mathfrak{p}|p$ be a finite prime of a number field K, and E an elliptic curve defined over K. In explicit terms, E can be given by a minimal Weierstrass equation with coefficients in $O_\mathfrak{p}$. In this way a continuous reduction map $\phi_\mathfrak{p} : E(K_\mathfrak{p}) \longrightarrow \overline{E}(k_\mathfrak{p})$, from $E(K_\mathfrak{p})$ to the finite set of points of the curve $\overline{E}$ described by the reduced Weierstrass equation over the residue class field $k_\mathfrak{p} = O/\mathfrak{p}$, is obtained. The set of points in the non-singular locus $\overline{E}^{\mathrm{ns}}(k_\mathfrak{p})$ of $\overline{E}$ is contained in the image of ϕ, by Hensel's lemma, and it inherits a natural group structure from $E(K_\mathfrak{p})$. Writing $E_0(K_\mathfrak{p}) = \phi^{-1}[\overline{E}^{\mathrm{ns}}(k_\mathfrak{p})]$, yields the exact sequence of topological groups

$$1 \to E_1(K_\mathfrak{p}) \longrightarrow E_0(K_\mathfrak{p}) \longrightarrow \overline{E}^{\mathrm{ns}}(k_\mathfrak{p}) \to 1. \tag{4}$$

The kernel of reduction $E_1(K_\mathfrak{p})$ is a subgroup of finite index in $E(K_\mathfrak{p})$.

For primes of good reduction, we have $E_0(K_\mathfrak{p}) = E(K_\mathfrak{p})$, and $\overline{E}^{\mathrm{ns}}(k_\mathfrak{p}) = \overline{E}(k_\mathfrak{p})$ is the point group of the elliptic curve $\overline{E} = (E \bmod \mathfrak{p})$ over $k_\mathfrak{p}$. For primes of bad reduction, $E_0(K_\mathfrak{p})$ is a strict subgroup of $E(K_\mathfrak{p})$, but it is of *finite* index in $E(K_\mathfrak{p})$ by [3, Chapter VII, Corollary 6.2.]

Lemma 3.2 *Let $T_\mathfrak{p}$ be the torsion subgroup of $E(K_\mathfrak{p})$. Then $T_\mathfrak{p}$ is a finite group, and $E(K_\mathfrak{p})/T_\mathfrak{p}$ is a free $\mathbb{Z}_p$-module of rank $[K_\mathfrak{p} : \mathbb{Q}_p]$.*

If $\mathfrak{p}$ is a prime of good reduction for E, then there exist an isomorphism

$$T_\mathfrak{p}^{non\text{-}p} \cong \overline{E}(k_\mathfrak{p})^{non\text{-}p}$$

between the maximal subgroups of $T_\mathfrak{p}$ and $\overline{E}(k_\mathfrak{p})$ that are of order coprime to $p = \mathrm{char}(k_\mathfrak{p})$.

Taking the product over all non-archimedean primes $\mathfrak{p}$ of K, and using the fact that the sum of the local degrees at the primes over p in K equals $[K : \mathbb{Q}]$, one gets the following.

Lemma 3.3 *For the group of adelic points of an elliptic curve E over a number field K, there is an isomorphism of topological groups*

$$E(\widehat{K}) = \widehat{\mathbb{Z}}^{[K:\mathbb{Q}]} \times \prod_{\mathfrak{p}} T_\mathfrak{p}, \tag{5}$$

with $T_\mathfrak{p} \subset E(K_\mathfrak{p})$ the finite torsion subgroup of $E(K_\mathfrak{p})$.

In order to describe *any* countable product T of cyclic groups, one can write each of the cyclic constituents of T as a product of cyclic groups of prime power order to arrive at the *standard representation*

$$T \cong \prod_{\ell \text{ prime}} \prod_{k=1}^{\infty} (\mathbb{Z}/\ell^k\mathbb{Z})^{e(\ell,k)}. \tag{6}$$

The exponents $e(\ell, k)$ can intrinsically be defined in terms of T as

$$e(\ell, k) = \dim_{\mathbb{F}_\ell} T[\ell^k]/\left(T[\ell^{k-1}] + \ell T[\ell^{k+1}]\right), \tag{7}$$

so any two groups written in this standard representation (6) are isomorphic if and only if their exponents $e(\ell, k)$ coincide for all prime powers ℓ^k.

The $\mathbb{F}_\ell$-dimensions $e(\ell, k)$ in (7) are either finite, in which case $e(\ell, k)$ is a non-negative integer, or countably infinite. In the latter case write $e(\ell, k) = \omega$. In the case where $e(\ell, k) = \omega$ for *all* prime powers ℓ^k, the group under consideration is

$$T_E = \prod_{m=1}^{\infty} \mathbb{Z}/m\mathbb{Z} \tag{8}$$

occurring in Theorem 2.1.

For the product $T = \prod_{\mathfrak{p}} T_{\mathfrak{p}}$ of local torsion groups at the finite primes $\mathfrak{p}$ that occurs in Lemma 3.3, the exponents $e(\ell, k)$, for the number of cyclic summands of prime power order in the standard representation (6) of T_E, have to be determined.

In the analogous situation of the closure T_K of the torsion subgroup of $\widehat{O}^*$ in [2, Section 2.3] that one had $e(\ell, k) = \omega$ for all but finitely many prime powers ℓ^k, and the 'missing' prime powers were characterized in terms of the number of exceptional roots of unity in K. In the elliptic situation, the cyclotomic extension of K generated by the ℓ^k-th roots of unity will be replaced by the ℓ^k-division field

$$Z_E(\ell^k) \stackrel{\text{def}}{=} K(E[\ell^k](\overline{K})) \tag{9}$$

of the elliptic curve E. This is the finite Galois extension of K obtained by adjoining the coordinates of all ℓ^k-torsion points of E to K. More precisely, the following holds:

Lemma 3.4 *Let E/K be an elliptic curve, and $\ell^k > 1$ a prime power for which the inclusion*

$$Z_E(\ell^k) \subset Z_E(\ell^{k+1})$$

of division fields is strict. Then $e(\ell, k) = \omega$ in the standard representation (6) *of the group T.*

It follows from Lemmas 3.3 and 3.4 that for elliptic curves E having the property that for all primes ℓ, the tower of ℓ-power division fields has strict inclusions

$$Z_E(\ell) \subsetneq Z_E(\ell^2) \subsetneq Z_E(\ell^3) \subsetneq \cdots \subsetneq Z_E(\ell^k) \subsetneq \cdots \tag{10}$$

at every level, the group T_E is the universal group $\prod_{m=1}^{\infty} \mathbb{Z}/m\mathbb{Z}$ for which $e(\ell, k) = \omega$ in the standard representation (6).

The structure of $E(\mathbf{A}_K)$ is determined by the Galois representation

$$\rho_E : \mathrm{Gal}(\overline{K}/K) \longrightarrow A = \mathrm{Aut}(E(\overline{K})^{\mathrm{tor}})$$

describing the action of the absolute Galois group of K by group automorphisms on the group $E(\overline{K})^{\mathrm{tor}}$ of all torsion points of E. The group A can be explicitly describe as

$$A = \mathrm{Aut}(E(\overline{K})^{\mathrm{tor}}) \cong \lim_{\leftarrow n} \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) = \mathrm{GL}_2(\widehat{\mathbb{Z}}),$$

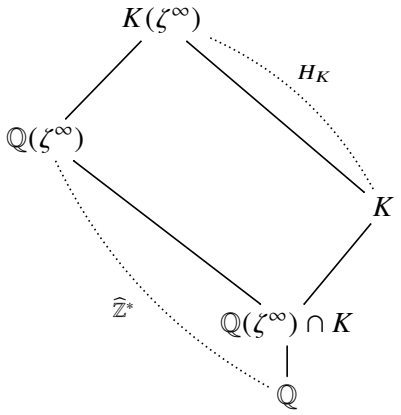
and ρ_E is a continuous homomorphism of profinite groups. The *image of Galois* for the representation ρ_E is the subgroup

$$G = \rho_E[\mathrm{Gal}(\overline{K}/K)] \subset A.$$

For $K = \mathbb{Q}$, Angelakis in [1, Section 4.4] uses a result of Nathan Jones to show that 'almost always' one has $E(\mathbb{A}_{\mathbb{Q}}) = \mathcal{E}$.

For $K \neq \mathbb{Q}$ using that $\mathrm{GL}_2(\widehat{\mathbb{Z}}) \xrightarrow{\det} \widehat{\mathbb{Z}}^*$ and denoting by H_K the Galois group $\mathrm{Gal}(K(\zeta^{\infty})/K)$ (see the figure below), it follows that the image $G \subset \det^{-1}[\mathrm{H_K}]$; this time, one can use the result of Zywina [4] to get that 'almost always' the image $G = \det^{-1}[\mathrm{H_K}]$, which implies that for every prime power $\ell^k > 1$ the inclusion $Z_E(\ell^k) \subset Z_E(\ell^{k+1})$ is strict. From Lemma 3.4 one gets that $e(\ell, k) = \omega$ for T in the standard representation (6). So putting (1), (3), (5) and (8) together, the group $E(\mathbb{A}_K)$ of adelic points of 'almost all' elliptic curves E/K, with n the degree of K, is isomorphic to the "generic group"

$$\mathcal{E} = (\mathbb{R}/\mathbb{Z})^n \times (\widehat{\mathbb{Z}})^n \times \prod_{m=1}^{\infty} \mathbb{Z}/m\mathbb{Z}. \tag{11}$$



References

[1] A. Angelakis, *Universal adelic groups for imaginary quadratic number fields and elliptic curves*, Leiden University & Université Bordeaux I, Doctoral Thesis, Leiden (2015)

[2] A. Angelakis, P. Stevenhagen, *Imaginary quadratic fields with isomorphic abelian Galois groups*, in *ANTS X - Proceedings of the Tenth Algorithmic Number Theory Symposium*, eds. Everett W. Howe and Kiran S. Kedlaya, The Open Book Series Vol 1, (2103) Mathematical Sciences Publisher, Berkeley, pp. 21-39.

[3] J.H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics vol. 106, Second Edition 2009, Springer, Dordrecht.

[4] D. Zywina, *Elliptic curves with maximal Galois action on their torsion points*, Bull. Lond. Math. Soc. **42** (2010), pp. 811-826

Athanasios Angelakis
Max Planck Institut für Mathematik
Vivatsgasse 7
53111 Bonn, Germany
email: math.angelakis@gmail.com

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 1, *Number* 1, *March* 2016, *pages* 17–21

Valerio Dose

Automorphisms of non-split Cartan modular curves

written by Mohammed Anwar

Modular curves are algebraic curves whose points (more precisely all but finitely many of them) parametrize families of elliptic curves. Classically modular curves are constructed as (compactifications of) quotients of the upper half plane under the action of subgroups of $\mathrm{SL}_2(\mathbb{Z})$. The general set up is as follows:

- $\mathfrak{h} = \{\tau \in \mathbb{C} : \mathrm{Im}(\tau) > 0\}$
- H a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$
- $\Gamma_H = \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) \mid \gamma \bmod N \text{ belongs to } H\}$

Then Γ acts on $\mathfrak{h}$ by fractional linear transformations:

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \quad \gamma(\tau) = \frac{a\tau + b}{c\tau + d}$$

and the action can be extended to $\mathfrak{h} \cup \mathbb{Q} \cup \{\infty\}$. The space of orbits $\mathfrak{h} \cup \mathbb{Q} \cup \{\infty\}/\Gamma_H$ can be given the structure of Riemann surface and is denoted by X_H and is called the *modular curve* associated to H. The point of X_H coming from $\mathbb{Q} \cup \{\infty\}$ are called the *cusps (or cuspidal points)* of X_H.

To connect the above definition to elliptic curves recall that to every $\tau \in \mathfrak{h}$ is associated a complex torus E_τ, (thus an elliptic curve over $\mathbb{C}$), defined by $E_\tau = \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z})$. Moreover any two such complex tori E_τ and $E_{\tau'}$ are isomorphic if and only if are in the same orbit under $\mathrm{SL}_2(\mathbb{Z})$. This gives the modular interpretation of X_Γ, (here $\Gamma = \mathrm{SL}_2(\mathbb{Z})$) as parametrizing isomorphism classes of elliptic curves. For general Γ_H one has to consider the following set up:

- E is an elliptic curve over $\mathbb{C}$, and $E[N]$ denotes the subgroup of N-torsion points.
- $\varphi : E[N] \to \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ is an isomorphism.
- Two pair (E, φ) and (E', φ') are equivalent if and only if there exist an isomorphism $f : E \to E'$, such that $M \circ \varphi = \varphi' \circ f$, for some $M \in H$.

Then, the non cuspidal points of X_H parametrize equivalence class of pairs (E, φ). A crucial fact is that the compact Rieman surfaces X_H can be given a structure of projective algebraic curve defined over the cyclotomic field $\mathbb{Q}(\zeta_N)$. Moreover if $\det : H \to \mathbb{Z}/NZ^*$ is surjective than X_H is actually defined over $\mathbb{Q}$.

One interesting problem is to study the group of automorphisms of X_H. Recall that $\mathrm{SL}_2(\mathbb{R})/\{\pm Id\}$ is the automorphisms group of $\mathfrak{h}$, acting upon $\mathfrak{h}$ by fractional linear transformations. If $N(\Gamma_H)$ denotes the the normaliser of Γ_H in $\mathrm{SL}_2(\mathbb{R})$, then an element η of $N(\Gamma_H)$ define an automorphism of $\mathfrak{h}/\Gamma_H$ and it can be shown that η extends to an automorphism of X_H. Set $B(X_H) = N(\Gamma_H)/\Gamma_H \subset \mathrm{Aut}(X_H)$, the elements of $B(X_H)$ are called *modular automorphisms*. A non-modular automorphism is called *exceptional*

Question 1 *When the genus of X_H is at least 2 is every automorphism of X_H modular?*

Beside being an interesting question on its own the above question is also related to Serre's Uniformity conjecture as follows: In [7] J.P.

Serre proved the following result (here and in the sequel CM stands for complex multiplication)

Theorem 2 *Let E be an elliptic curve over $\mathbb{Q}$. If E is without CM then there exist a constant C_E such that for every prime number $p > C_E$ the Galois representation modulo p attached to E is surjective.*

Serre asked whether the constant C_E could be made independent of E:

Question 3 (Serre's uniformity problem) *Does there exist a number C_0 such that for every elliptic curve without CM and every $p > C_0$ the Galois representations modulo p attached to E is surjective?*

It widely believed that one can take $C_0 = 37$, (see, e.g. [1]). Since the maximal subgroup of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ are:

- Exceptional subgroups, i.e. those whose image in $\mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$ is isomorphic to $\mathcal{A}_4$, $\mathcal{S}_4$, or $\mathcal{A}_5$.
- Borel subgroups.
- Normalizers of split Cartan subgroups.
- Normalizers of non-split Cartan subgroups.

Thus, to solve Serre's uniformity problem, one has to prove that for sufficiently large p the image of the Galois representation is not contained in any of the above subgroups. Serre settled the exceptional subgroups, while the case of Borel subgroups follows from work of Mazur [6] on rational isogenies of prime degree. Much more recently Bilu and Parent solved Serre's problem in the split Cartan case. Thus the only remaining case is the non-split Cartan.

The connection to points on modular goes as follows: Let H be a (maximal) subgroup of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$, then a rational point on X_H is associated to a pair (E, φ), where

- E is an elliptic curve defined over $\mathbb{Q}$;

- $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on the p-torsion to as subgroup of H;
- the image of the Galois representation modulo p attached to E is contained in H.

We refer the interested reader to [5] for details.
Thus elliptic curves without CM, for which the associate Galois representation modulo p is not surjective correspond to (non CM) rational points on the modular curve X_H (for some maximal subgroup H of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$), which are not cusps. Such a rational point could be constructed as the mage of a cuspidal point via an exceptional automorphism of X_H.

Let C be a non-split Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ and C^+ its normalizer. The associated modular curves are denoted by $X_{ns}(p)$ and $X_{ns}^+(p)$ respectively. C has index 2 in C^+ and there exists a degree two morphism $X_{ns}(p) \to X_{ns}^+(p)$ and a modular involution w of $X_{ns}^+(p)$, such that $X_{ns}^+(p) = X_{ns}(p)/\langle w\rangle$. Moreover $B\left(X_{ns}(p)\right) = \langle w\rangle$ and $B\left(X_{ns}^+(p)\right)$ is trivial. It is expected that for large p all the automorphism of $X_{ns}(p)$ are modular. The following are some recent result on regarding the automorphism group of $X_{ns}(p)$

Theorem 4 ([2]) *The automorphism group of $X_{ns}(11)$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2Z$.*

Theorem 5 ([3])

1) For $p \geq 37$ all the automorphisms of $X_{ns}(p)$ preserve the cusps.

2) If $p \equiv 1 \bmod 12$ and $p \neq 13$, then

$$\mathrm{Aut}(X_{ns}(p)) = \langle w\rangle = B\left(X_{ns}(p)\right)$$

Theorem 6 ([4]) *If $13 \leq p \leq 31$, then*

1) $\mathrm{Aut}(X_{ns}^+(p))$ *is trivial.*

2) $\mathrm{Aut}(X_{ns}(p)) = \langle w\rangle$

References

[1] Y. Bilu and P. Parent *Serre's uniformity problem in the split Cartan case*, Ann. of Math. 2 Vol 173 (2011), pp. 569-584.

[2] V. Dose, J. Fernández, J. González and R. Schoof,*The automorphism group of the non-split Cartan modular curve of level 11*, J. Algebra, 417 (2014) p.95-102.

[3] V. Dose, *On the automorphisms of the non-split cartan modular curves of prime level*, arXiv:1503.05165.

[4] J. González *Constraints on the automorphism group of a curve*, arXiv:1503.05691.

[5] B. Mazur *Rational points on modular curves*, in Modular functions of one variable V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976), pp. 107-148; Lecture Notes in Math. 601, Springer, Berlin, 1977.

[6] B. Mazur, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math. 44 (1978), pp. 129-162.

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

Mohammed Anwar
Dipartimento di Matematica e Fisica
Università Roma Tre
L.go San Leonardo Murialdo 1
00146 Roma, Italy.
email: anwar@mat.uniroma3.it

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 1, *Number* 1, *March* 2016, *pages* 23–27

Christian Mauduit

Automata and Number Theory

written by Valerio Dose

Many natural questions in number theory arise from the study of the multiplicative representations of integers, and they are often at the origin of many important open problems in Mathematics and Computer Science. Among these questions, a simpler family consists of those which can be formulated by means of functions defined using an algorithm which is "simple" enough, in a way that will be made clear below.

The study of a finite number of subsets of the natural numbers $\mathbb{N}$, can be related to the study of sequences of symbols in a finite set. For example, we can associate to even and odd numbers the set of symbols $\{0, 1\}$ and the infinite sequence $010101\ldots$. Also, we can associate to any subset $E \subseteq \mathbb{N}$ and to any integer $q \geq 2$, the language

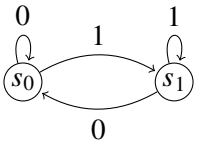
$$L_q(E) = \{\mathrm{rep}_q(n), n \in E\}$$

where $\mathrm{rep}_q(n)$ is the representation of n in base q, which makes $L_q(E)$ a set of words on the alphabet $\{0, 1, \ldots, q-1\}$. This relation allows to express many questions about arithmetic sequences in the framework of the theory of formal languages, thus establishing a link between number theory, language theory and combinatorics on words.

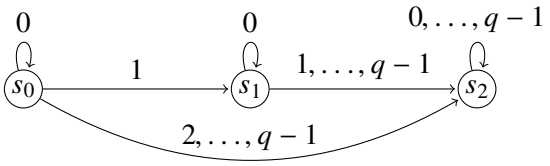
In virtue of this connection, it is interesting to consider automatic sequences of integers, which are those recognizable by finite automata

(an introduction to finite automata can be found in the book of Allouche and Shallit [1]).

For example, the graph associated to the finite 2-automaton that recognizes even numbers represented in base 2 and read from the left to the right can be represented by the diagram:



where s_0 is the initial and unique final state. A more elaborated example if given by the graph associated to the finite q-automaton that recognizes numbers in the sequence $\{q^n, n \in \mathbb{N}\}$, written in base q:



where s_0 is the initial state and s_1 is the unique final state.

A fundamental result that relates Number Theory to Finite Automata was proven if 1980:

Theorem 1 (Christol, Kamae, Mendès France and Rauzy, [2]) *Let $E \subseteq \mathbb{N}$ and $\mathbb{F}_q$ a finite field. The formal power series*

$$\sum_{n \in E} X^{-n} \in \mathbb{F}_q\left(\left(X^{-1}\right)\right)$$

is algebraic over $\mathbb{F}_q(X)$ if and only if E is recognizable by a finite q-automaton.

To understand how simple automatic sequences are, we define, for any sequence $w = \{w_n\}_{n\in\mathbb{N}}$ on a finite alphabet A, the function $p_w : \mathbb{N} \to \mathbb{N}$ by

$$p_w(n) = \#\{(b_1, \ldots, b_n), \exists k \text{ s.t. } w_k = b_1, \ldots, w_{k+n+1} = b_n\}$$

(i.e. $p_w(n)$ is the number of distinct factors of lenght n in the sequence w).

The connection between automaton and the function p_w was established in 1972:

Theorem 2 (Cobham [3]) *If w is recognizable by a finite q-automaton, then $p_w(n) = O(n)$.*

From a number theoretic point of view, it is a natural question to ask whether is it possible to recognize prime numbers with a finite automaton. The answer to this question is negative, as shown by Minsky and Papert (1966), in a result then generalized by Hartmanis, Shank and Schützenberger (1968), by Mauduit (1992) and by Cassaigne and Le Gonidec (2006).

Other natural questions regard the existence of prime numbers in a given automatic sequence. For examples the sequences $\{2^n + 1\}_{n\in\mathbb{N}}$ and $\{2^n - 1\}_{n\in\mathbb{N}}$ are both recognizable by a finite 2-automaton, and the problems associated correspond respectively to the search of Fermat and Mersenne primes.

In the case when E is a set recognized by a finite automaton whose associated graph is strongly connected, it follows from a remark by Fouvry and Mauduit (1996) that E contains infinitely many almost primes (see [4]). On the other hand it is still an open problem to find an asymptotic estimate for the number of primes less than a certain bound x in the set E.

For general automatic sets the situation is more complicated. One of the first problems to be considered in this direction concerns the search of primes with missing digits. Though some results on integers with

missing digits were obtained by Erdős, Mauduit and Sárközy (1998), the problem of finding an asymptotic estimate of the quantity

$$\#\{p \leq x,\, p \text{ prime}, \operatorname{rep}_q(p) \in D^*\}$$

where D^* is the set of words on any given subset $D \subset \{0, \ldots, q-1\}$, is still open.

Other famous automatic sequences are the Thue-Morse sequences and the Rudin-Shapiro sequences. For these two examples it can be proved the following results appeared respectively in 2010 and 2015 (see also [5]):

Theorem 3 (Mauduit and Rivat [6]) *Let*

$$(t_n)_{n\in\mathbb{N}} = 01101001100101101001011001101001\ldots$$

be the Thue-Morse sequence and let $\mathbb{P}$ be the set of prime numbers. The frequences of 0 and 1 in the sequence $(t_p)_{p\in\mathbb{P}}$ is $\dfrac{1}{2}$.

Theorem 4 (Mauduit and Rivat [7]) *Let*

$$(r_n)_{n\in\mathbb{N}} = 00010010000111010001001 0\ldots$$

be the Rudin-Shapiro sequence and let $\mathbb{P}$ be the set of prime numbers. The frequences of 0 and 1 in the sequence $(r_p)_{p\in\mathbb{P}}$ is $\dfrac{1}{2}$.

References

[1] J.-P. Allouche and J. Shallit, *Automatic sequences*, Cambridge University Press, Cambridge, 2003. Theory, applications, generalizations.

[2] G. Christol, T. Kamae, M. Mendès France, and G. Rauzy, *Suites algébriques, automates et substitutions*, Bull. Soc. Math. France, **108** n. 4, 401–419 (1980).

[3] A. Cobham, *Uniform tag sequences*, Math. Systems Theory **6**, 164–192 (1972).

[4] E. Fouvry and C. Mauduit. *Sommes des chiffres et nombres presque premiers*, Math. Ann. **305** n. 3, 571–599 (1996).

[5] B. Martin, C. Mauduit, and J. Rivat, *Théorème des nombres premiers pour les fonctions digitales*, Acta Arith. **165** n. 1, 11–45 (2014).

[6] C. Mauduit and J. Rivat, *Sur un problème de Gelfond: la somme des chiffres des nombres premiers*, Ann. of Math. (2), **171** n. 3, 1591–1646 (2010).

[7] C. Mauduit and J. Rivat, *Prime numbers along Rudin-Shapiro sequences*, J. Eur. Math. Soc., **17** 2595–2642 (2015).

Valerio Dose
Dipartimento di Matematica
Università di Roma "Tor Vergata"
Via della Ricerca Scientifica 1
00133 Roma, Italy
e-mail address: dose@mat.uniroma2.it

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 1, *Number* 1, *March* 2016, *pages* 29–35

Nathan Jones

The distribution of class groups of imaginary quadratic fields

written by Giulio Meleleo

The study of class groups and of class numbers has been a central task in number theory since their introduction, around 1845, by Kummer. The interest for the class group of imaginary quadratic fields goes actually back to Gauss, who in [2, art. 303-304], already predicted that there exists only finitely many imaginary quadratic number fields having a given class number and asked for a complete list of such number fields for each given value. Evidently Gauss formulated his result and conjecture in terms of quadratic forms. in 1934 Heilbron [3] established Gauss claim, by proving that the class number of imaginary quadratic number tends to infinity as the discriminant grows, and thus proving that every finite abelian group can appear as the class group of an imaginary quadratic field only finitely many times. It is then only natural to ask the following:

Question 1 *Let G be a finite abelian group. How many times does G occur as the class group of some imaginary quadratic field?*

Set

$$\mathcal{F}(G) := \#\{\text{imaginary quadratic fields } K \,:\, \mathrm{cl}(\mathcal{O}_K) \simeq G\}.$$

The following table is made out of a (much larger) set of data obtained by computations carried out with the aid of a supercomputer and under the GRH (cf. [4]):

p	3	5	7	11	13	17	19	23
$\mathcal{F}\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)$	33	93	130	241	335	518	599	823
$\mathcal{F}\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\times\frac{\mathbb{Z}}{p\mathbb{Z}}\right)$	1	2	2	0	5	1	0	1

Looking at the table it is natural to ask if $\mathcal{F}\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\times\frac{\mathbb{Z}}{p\mathbb{Z}}\right) > 0$ for infinitely many primes p. Evidently one can ask similar questions for groups of order p^n, for any $n \geq 2$. To formulate a precise question we need a little bit of notation. Let p be an odd prime. As it is well know isomorphism classes of abelian groups of order p^n are in one-to-one correspondence with the set of all possible partitions of n. Namely

$$\begin{aligned}\{[G] : G \text{ abelian group}, |G| = p^n\} &\leftrightarrow \mathrm{Part}(n)\\ \bigoplus_{i=1}^{k} \mathbb{Z}/p^{n_i}\mathbb{Z} &\mapsto (n_1, \ldots, n_k)\end{aligned}$$

where

$$\mathrm{Part}(n) = \left\{(n_1, \ldots, n_k) \in \mathbb{N}^k : \sum_{i=1}^{k} n_1{=}n,\ n_1{\geq}n_2{\geq}\cdots{\geq}n_k\right\}.$$

If $\lambda := (n_1, \ldots, n_k) \in \mathrm{Part}(n)$, we denote with $G_\lambda(p^n)$ the corresponding abelian group. Thus we can formulate the following

Question 2 *Is $\mathcal{F}\left(G_\lambda(p^n)\right) > 0$ for infinitely many primes p?*

Given $\lambda = (n_1, \ldots, n_k) \in \mathrm{Part}(n)$ let

$$\mathrm{cyc}(\lambda) := n_1 - \sum_{i=2}^{k}(2i-3)n_i.$$

Note that $1-(n-1)^2 \leq \mathrm{cyc}(\lambda) \leq n$ and is equal to n if and only if $G_\lambda(p^n)$ is cyclic.

Conjecture 3 (Holmin, Kurlberg, Jones, McLeman, Petersen) *Fix $n \in \mathbb{N}$ and $\lambda \in \mathrm{Part}(n)$. As $x \to \infty$, one has*

$$\sum_{p \leq x} \mathcal{F}(G_\lambda(p^n)) = \begin{cases} \frac{15C}{n(\mathrm{cyc}(\lambda)+1)} \cdot \frac{x^{\mathrm{cyc}(\lambda)+1}}{(\log x)^2}(1+o(1)) & \mathrm{cyc}(\lambda) \geq 0 \\ O(1) & \mathrm{cyc}(\lambda) < 0. \end{cases}$$

where C is defined by the Euler product

$$C := \prod_{\substack{\ell=3 \\ \ell \text{ prime}}}^{\infty} \prod_{i=2}^{\infty} \left(1 - \frac{1}{\ell^i}\right) \approx 0.754\ldots$$

It is interesting to see explicitly what the conjecture says for $n = 2, 3$.

$\boxed{n=2}$

Consider the partition $\lambda = (1,\ 1)$, for which $\mathrm{cyc}(1,\ 1) = 0$, we have the following set of data

p	3	5	7	11	13	17	19	23
$\mathcal{F}\left(\frac{\mathbb{Z}}{p\mathbb{Z}} \times \frac{\mathbb{Z}}{p\mathbb{Z}}\right)$	1	2	2	0	5	1	0	1

The conjecture asserts that as $x \to \infty$,

$$\sum_{p \leq x} \mathcal{F}\left(\frac{\mathbb{Z}}{p\mathbb{Z}} \times \frac{\mathbb{Z}}{p\mathbb{Z}}\right) \sim \frac{15C}{2} \frac{x}{(\log x)^2}$$

In particular is expected that $\mathcal{F}\left(\frac{\mathbb{Z}}{p\mathbb{Z}} \times \frac{\mathbb{Z}}{p\mathbb{Z}}\right) > 0$ for an infinite set of primes (of asymptotic density zero)

$\boxed{n=3}$

Consider the two partitions $(1,\ 2)$ ($\mathrm{cyc}(2,\ 1) = 1$) and $(1,\ 1,\ 1)$ ($\mathrm{cyc}(1,\ 1,\ 1) = -3$) , in this case the data collected in [4]) gives:

p	3	5	7	11	13	17	19
$\mathcal{F}\left(\frac{\mathbb{Z}}{p^2\mathbb{Z}} \times \frac{\mathbb{Z}}{p\mathbb{Z}}\right)$	5	11	13	19	17	25	22
$\mathcal{F}\left(\frac{\mathbb{Z}}{p\mathbb{Z}} \times \frac{\mathbb{Z}}{p\mathbb{Z}} \times \frac{\mathbb{Z}}{p\mathbb{Z}}\right)$	0	0	0	0	0	0	0

The conjecture asserts that as $x \to \infty$,

$$\sum_{p \leq x} \mathcal{F}\left(\frac{\mathbb{Z}}{p^2\mathbb{Z}} \times \frac{\mathbb{Z}}{p\mathbb{Z}}\right) \sim \frac{15C}{8} \frac{x^2}{(\log x)^2}$$

whereas

$$\sum_{p \leq x} \mathcal{F}\left(\frac{\mathbb{Z}}{p\mathbb{Z}} \times \frac{\mathbb{Z}}{p\mathbb{Z}} \times \frac{\mathbb{Z}}{p\mathbb{Z}}\right) \sim O(1)$$

The heuristic behind the conjecture is based on the Cohen-Lenstra heuristic for class groups (cf. [1]). Given G, set

$$P(G) := \frac{1/|\operatorname{Aut}(G)|}{\sum_{|H|=|G|} 1/|\operatorname{Aut}(H)|},$$

Then Cohen-Lenstra heuristic predicts that the probability of G being the class group of an imaginary quadratic field is exactly $P(G)$.

Let

$$\mathcal{F}(h) := \#\{\text{imaginary quadratic fields } K : |cl(\mathcal{O}_K)| = h\}.$$

So that $\mathcal{F}(h) = \sum_{|G|=h} \mathcal{F}(G)$, where the sum runs over the isomorphism classes of abelian groups of order h. By the Cohen-Lenstra heuristic one expects to have

$$\mathcal{F}(G_\lambda(p^n)) \approx P(G_\lambda(p^n)) \cdot \mathcal{F}(p^n).$$

In 1907, Ranum proved that for $\lambda \in \operatorname{Part}(n)$, one has $P(G_\lambda(p^n)) \sim p^{\operatorname{cyc}(\lambda)-n}$ for p that tends to infinity (see [5]). Moreover, a recent

conjecture of Soundararajan [6] says that for $h \to \infty$ through odd values, $\mathcal{F}(h) \asymp \frac{h}{\log h}$. Hence, we can deduce that

$$\mathcal{F}(G_\lambda(p^n)) \approx p^{\mathrm{cyc}(\lambda)-n} \cdot \frac{p^n}{\log(p^n)} = \frac{p^{\mathrm{cyc}(\lambda)}}{n \log p}.$$

Finally, we can see that

$$\sum_{p \le x} \mathcal{F}(G_\lambda(p^n)) \approx \sum_{p \le x} \frac{p^{\mathrm{cyc}(\lambda)}}{n \log p} \sim \frac{1}{n(\mathrm{cyc}(\lambda)+1)} \cdot \frac{x^{\mathrm{cyc}(\lambda)+1}}{(\log x)^2}.$$

This is, up to a the multiplicative constant $15C$ the content of Conjecture 3. The presence of $15C$ can be explained via the following refinement of Soundararajan's conjecture:

Conjecture 4 (Holmin, Kurlberg, Jones, McLeman, Petersen) *For $h \to \infty$ through odd values,*

$$\mathcal{F}(h) \sim 15 \cdot C \cdot c(h) \cdot \frac{h}{\log h}$$

where

$$c(h) = \prod_{p^n \,||\, h}^{\infty} \prod_{i=1}^{n} \left(1 - \frac{1}{p^i}\right)^{-1}$$

Another important theorem of Soundararajan [6] says that for $H \to \infty$, one has

$$\frac{1}{H} \sum_{h \le H} \mathcal{F}(h) \sim \frac{3\zeta(2)}{\zeta(3)} H.$$

A result related to this one is the following:

Theorem 5 (Holmin, Kurlberg, Jones, McLeman, Petersen) *Assume the Generalize Riemann Hypothesis. Then*

$$\frac{1}{H/2} \sum_{\substack{h \le H \\ h \ odd}} \mathcal{F}(h) \sim \frac{\pi^2 \zeta(2)}{\zeta(4)} \cdot \frac{H}{\log H}$$

for $H \to \infty$.

Lastly one can ask if a "typical" $G_\lambda(p^n)$ satisfies $\mathcal{F}(G_\lambda(p^n)) > 0$ infinitely often. An answer to this question is the following result.

Theorem 6 (Holmin, Kurlberg, Jones, McLeman, Petersen)

$$\frac{\#\{\lambda \in \mathrm{Part}(n) : \mathrm{cyc}(\lambda) \geq 0\}}{\#\,\mathrm{Part}(n)} \ll n^{5/4} e^{(2-\pi\sqrt{2/3})\sqrt{n}}.$$

In particular, almost all partitions $\lambda \in \mathrm{Part}(n)$ *conjecturally satisfy* $\mathcal{F}(G_\lambda(p^n)) = 0$ *for* $p \gg 1$.

The proof of this theorem is combinatorial, via generating functions.

For all the results highlighted in this extended abstract we refer the reader to [4].

References

[1] H. Cohen, and H.W. Lenstra, *Heuristics on class groups of number fields*, Number theory, Noordwijkerhout 1983, Lecture Notes in Math., vol. 1068, Springer, Berlin, 1984, pp. 33-62

[2] C. F. Gauss, *Disiquisitiones Artithmeticae*, English Editon, Translated by Arthur A. Clarke, Springer-Verlag, New York, 1986.

[3] H. Heilbronn, *On the Class Number in Imaginary Quadratic Fields*, Quart. J. Math. Oxford Ser. 25, 150-160, 1934.

[4] S. Holmin, N. Jones, P. Kurlberg, P. McLeman, and K. Petersen, *Missing class groups and class number statistics for imaginary quadratic fields*, preprint.

[5] A. Ranum, *The group of classes of congruent matrices with application to the group of isomorphisms of any abelian group*, Trans. Amer. Math. Soc. 8 (1907), 71–91.

[6] K. Soundararajan, *The number of imaginary quadratic fields with a given class number*, Hardy-Ramanujan J. 30 (2007), 13–18.

Giulio Meleleo
Dipartimento di Matematica e Fisica
Università Roma Tre
L.go San Leonardo Murialdo 1
00146 Roma, Italy.
email: meleleo@mat.uniroma3.it

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 1, *Number* 1, *March* 2016, *pages* 37–41

Alina Ostafe

On some extensions of the Ailon-Rudnick Theorem

written by Lorenzo Menici

Let $a, b \in \mathbb{N}_{\geq 2}$ be multiplicatively independent in $\mathbb{Q}^*$. The quantity $\gcd(a^n - 1, b^n - 1)$, $n \in \mathbb{N}$, has been investigated by several authors. An important result was obtained by Bugeaud, Corvaja and Zannier [3], who proved that for any $\epsilon > 0$,

$$\gcd(a^n - 1, b^n - 1) \leq \exp(\epsilon n) ,$$

as n tends to infinity.

The function field analogue, given $f, g \in \mathbb{C}[X]$, corresponds to finding upper bounds for $\deg \gcd(f^n - 1, g^n - 1)$. The following definition is central for the next results.

Definition 1 *The polynomials $F_1, \ldots, F_s \in \mathbb{C}[X_1, \ldots, X_\ell]$ are multiplicatively independent if there exists no nonzero vector $(\nu_1, \ldots, \nu_s)$ in $\mathbb{Z}^s$ such that*

$$F_1^{\nu_1} \cdots F_s^{\nu_s} = 1.$$

Similarly, the polynomials $F_1, \ldots, F_s \in \mathbb{C}[X_1, \ldots, X_\ell]$ are multiplicatively independent in the group $\mathbb{C}(X_1, \ldots, X_\ell)^*/\mathbb{C}^*$ if there exists no nonzero vector $(\nu_1, \ldots, \nu_s) \in \mathbb{Z}^s$ and $a \in \mathbb{C}^*$ such that

$$F_1^{\nu_1} \cdots F_s^{\nu_s} = a.$$

Ailon and Rudnick [1] showed that for multiplicatively independent polynomials $f, g \in \mathbb{C}[X]$, there exists $h \in \mathbb{C}[X]$ such that

$$\gcd(f^n - 1, g^n - 1) \mid h \tag{1}$$

for all $n \geq 1$. If in addition $\gcd(f - 1, g - 1) = 1$, then there is a finite union of arithmetic progressions $\cup_{d_i}\mathbb{N}$, $d_i \geq 2$, such that, for n outside these progressions, $\gcd(f^n - 1, g^n - 1) = 1$.

Corvaja and Zannier [4] extended the result of Ailon and Rudnick [1] to S-units: let $S \subset \mathbb{C}$ be a finite set and let $u, v \in \mathbb{C}(X)$ be multiplicatively independent rational functions with all their zeroes and poles in S. Then

$$\deg \gcd(u - 1, v - 1) \ll \max(\deg u, \deg v)^{2/3}. \tag{2}$$

As a corollary, if $f, g \in \mathbb{C}[X]$ are multiplicatively independent, then one gets $\deg \gcd(f^n - 1, g^n - 1) \ll n^{2/3}$, which improves the trivial bound $\ll n$.

In [5] several extensions of the Ailon-Rudnick theorem over $\mathbb{C}$ are developed in order to study:

1. $\gcd\left(h_1(f^n), h_2(g^m)\right)$, where $h_1, h_2 \in \mathbb{C}[X]$;
2. $\gcd\left(f_1^{n_1} \cdots f_\ell^{n_\ell} - 1, g_1^{m_1} \cdots g_r^{m_r} - 1\right)$, where $f_1, \ldots, f_\ell$ and $g_1, \ldots, g_r$ belong to $\mathbb{C}[X]$;
3. $\gcd\left(h_1(F^n), h_2(G^m)\right)$, where $h_1, h_2 \in \mathbb{C}[X]$ and both F and G belong to $\mathbb{C}[X_1, \ldots, X_m]$;
4. the set of common zeros of $F_1^{n_1} - 1, \ldots, F_{\ell+1}^{n_{\ell+1}} - 1$ over $\mathbb{C}$, which is denote by $Z\left(F_1^{n_1} - 1, \ldots, F_{\ell+1}^{n_{\ell+1}} - 1\right)$, where $F_1, \ldots, F_{\ell+1} \in \mathbb{C}[X_1, \ldots, X_\ell]$.

The goal is to obtain uniform bounds for the degree of these gcd's in the sense that they do not depend on the powers $n, m, \ldots$.

Using a uniform bound for the number of points on a curve with coordinates roots of unity due to Beukers and Smyth [2], one obtains

an upper bound on $\deg \gcd(f^n-1, g^m-1)$ that depends only the degrees of f and g:

Lemma 1 *Let $f, g \in \mathbb{C}[X]$ be non constant polynomials. If f and g are multiplicatively independent, then*

$$\deg \gcd\left(f^n - 1, g^m - 1\right) \leq \left(11(d_f + d_g)^2\right)^{\min(d_f, d_g)}.$$

for all $n, m \geq 1$.

This result can be generalized to:

Theorem 2 *Let $f, g, h_1, h_2 \in \mathbb{C}[X]$. If f and g are multiplicatively independent in $\mathbb{C}(X)^*/\mathbb{C}^*$, then*

$$\deg \gcd\left(h_1\left(f^n\right), h_2\left(g^m\right)\right) \leq d_{h_1} d_{h_2} \left(11(d_f + d_g)^2\right)^{\min(d_f, d_g)}.$$

for all $n, m \geq 1$.

Another extension of the Ailon-Rudnick theorem obtained in [5] is the following:

Theorem 3 *Let $f_1, \ldots, f_\ell, g_1, \ldots, g_r \in \mathbb{C}[X]$, $\ell, r \geq 1$, be multiplicatively independent polynomials. Then, for all $n_1, \ldots, n_\ell, m_1, \ldots, m_r \geq 1$, there exists a polynomial $h \in \mathbb{C}[X]$ such that*

$$\gcd\left(f_1^{n_1} \cdots f_\ell^{n_\ell} - 1, g_1^{m_1} \cdots g_r^{m_r} - 1\right) \mid h.$$

If in addition

$$\gcd(f_1 \cdots f_\ell - 1, g_1 \cdots g_r - 1) = 1,$$

then there exists a finite number of monoids $\mathcal{L}_s$ in $\mathbb{N}^{\ell+r}$ such that $\mathbb{N}^{\ell+r} \setminus \cup_s \mathcal{L}_s$ is infinite and for any vector $(n_1, \ldots, n_\ell, m_1, \ldots, m_r) \in \mathbb{N}^{\ell+r} \setminus \cup_s \mathcal{L}_s$,

$$\gcd\left(f_1^{n_1} \cdots f_\ell^{n_\ell} - 1, g_1^{m_1} \cdots g_r^{m_r} - 1\right) = 1.$$

Theorem 3 can also be reformulated in terms of S-units in $\mathbb{C}[X]$ and gives a uniform bound for $\deg \gcd(u-1, v-1)$. Such a uniform bound is not present in (2) which, on the other hand, applies to more general situations.

It might be possible to unify Theorems 2 and 3 to obtain a similar result for

$$\gcd\left(h_1\left(f_1^{n_1}\cdots f_\ell^{n_\ell}\right), h_2\left(g_1^{m_1}\cdots g_r^{m_r}\right)\right),$$

where $h_1, h_2 \in \mathbb{C}[X]$. Similar ideas may work for this case however they require a uniform bound for the number of points on intersections of curves in the torus $\mathbb{G}_m^{\ell+r}$ with algebraic subgroups of dimension $k \leq \ell + r - 2$, which is not available. This will also give a bound for $\deg h$ in Theorem 3.

In the multivariate case, applying Hilbert's Irreducibility Theorem to reduce via specializations to the univariate case, we get:

Theorem 4 *Let $h_1, h_2 \in \mathbb{C}[X]$ and $F, G \in \mathbb{C}[X_1, \ldots, X_\ell]$. We denote by*

$$D = \max_{i=1\ldots,\ell}\left(\deg_{X_i} F, \deg_{X_i} G\right).$$

If F, G are multiplicatively independent in $\mathbb{C}(X_1, \ldots, X_\ell)^*/\mathbb{C}^*$, then for all $n, m \geq 1$ we have

$$\deg \gcd\left(h_1\left(F^n\right), h_2\left(G^m\right)\right) \leq d_{h_1} d_{h_2}\left(44(D+1)^{2\ell}\right)^{(D+1)^\ell}.$$

Lastly, for an integer $D \geq 1$, if we denote $\gamma_\ell(D) = \binom{\ell+1+D^\ell}{\ell+1}$, then we have the following result:

Theorem 5 *Let $F_1, \ldots, F_{\ell+1} \in \mathbb{C}[X_1, \ldots, X_\ell]$ be multiplicatively independent polynomials of degree at most D. Then,*

$$\bigcup_{n_1,\ldots,n_{\ell+1}\in\mathbb{N}} Z\left(F_1^{n_1} - 1, \ldots, F_{\ell+1}^{n_{\ell+1}} - 1\right)$$

is contained in at most

$$N \leq \left(0.792\gamma_\ell(D)/\log\left(\gamma_\ell(D)+1\right)\right)^{\gamma_\ell(D)}$$

algebraic varieties, each defined by at most $\ell + 1$ polynomials of degree at most

$$(\ell + 1)D^{\ell} \prod_{p \leq \gamma_{\ell}(D)} p$$

(the product runs over all primes $p \leq \gamma_{\ell}(D)$).

References

[1] N. Ailon and Z. Rudnick, *Torsion points on curves and common divisors of $a^k - 1$ and $b^k - 1$*, Acta Arith., **113** (2004), no. 1, 31–38.

[2] F. Beukers and C. J. Smyth, *Cyclotomic points on curves*, Number Theory for the Millenium (Urbana, Illinois, 2000), I, A K Peters, 2002, 67–85.

[3] Y. Bugeaud, P. Corvaja and U. Zannier, *An upper bound for the G.C.D. of $a^n - 1$ and $b^n - 1$*, Math. Z., **243** (2003), 79–84.

[4] P. Corvaja and U. Zannier, *Some cases of Vojtas conjecture on integral points over function fields*, J. Alg. Geom., **17** (2008), 295–333.

[5] A. Ostafe, *On some extensions of the Ailon-Rudnick Theorem*, `arXiv:1505.03957` (2015).

Lorenzo Menici,
Dipartimento di Matematica e Fisica
Università Roma Tre
L.go San Leonardo Murialdo 1
00146, Roma Italy.
email: `menici@mat.uniroma3.it`

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 1, *Number* 1, *March* 2016, *pages* 43–48

Leonardo Zapponi

Parametric Solutions of Pell's Equation

written by Pietro Mercuri

1 Introduction

An *ordinary Pell's equation* is an equation of the form

$$x^2 - ny^2 = 1, \tag{1}$$

where n is a positive integer that is not a square. It is well known that a pair of integers (x, y) is a solution for (1) if and only if $x + y\sqrt{n}$ is a unit with norm 1 of the ring $\mathbb{Z}[\sqrt{n}]$. It is also known that the integer solutions of (1) form an abelian group V isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$. Moreover, $V \cap \mathbb{R}_{>0} \cong \mathbb{Z}$ is cyclic and a generator of this group is called a fundamental solution of (1).

A *polynomial Pell's equation* is an equation of the form

$$P^2 - DQ^2 = 1, \tag{2}$$

where $D \in \mathbb{Z}[X]$ is not a square. We are interested in solutions $P, Q \in \mathbb{Z}[X]$. Now, we define what a parametric solution of a Pell's equation is. Let the pair (a, b) be a fundamental solution of the ordinary Pell's equation (1). A pair (P, Q), with $P, Q \in \mathbb{Z}[X]$, is a *parametric solution*

associated to (a, b) if there is a polynomial $D \in \mathbb{Z}[X]$ that is not a square and $\deg(D) = 2$ such that (P, Q) is a solution of (2) and there is an integer k such that

$$\begin{cases} P(k) = a, \\ Q(k) = b, \\ D(k) = n. \end{cases}$$

The *degree* of a parametric solution (P, Q) associated to (a, b) is $\deg(P)$. Without loss of generality we can assume that $k = 0$. With this assumption, if the polynomials $P, Q, D \in \mathbb{Z}[X]$ form a parametric solution, then $P(mX), Q(mX), D(mX)$ form a parametric solution for every nonzero integer m. From now on, we also assume that $\deg(D) = 2$.

The solutions of a Pell's equation are strictly related to Chebyshev polynomials. Let V be the $\mathbb{C}(X)$-vector space of sequences $\{u_n\}_{n\in\mathbb{N}}$, with $u_n \in \mathbb{C}(X)$ such that

$$u_{n+1} = 2Xu_n - u_{n-1}.$$

We know that V has dimension 2 and a basis is $\{T_n, U_n\}$, where $T_n, U_n \in \mathbb{Z}[X]$ are the *Chebyshev polynomials of first and second kind of degree* n respectively. They are defined by

$$\begin{cases} T_0(X) = 1 \\ T_1(X) = X, \end{cases} \quad \text{and} \quad \begin{cases} U_0(X) = 1 \\ U_1(X) = 2X. \end{cases}$$

Explicitly they can be expressed as

$$T_n(X) = \frac{1}{2}\left[\left(X - \sqrt{X^2-1}\right)^n + \left(X + \sqrt{X^2-1}\right)^n\right],$$
$$U_n(X) = \frac{1}{2\sqrt{X^2-1}}\left[\left(X - \sqrt{X^2-1}\right)^{n+1} - \left(X + \sqrt{X^2-1}\right)^{n+1}\right],$$

and, in the field $\mathbb{C}(X)\left[\sqrt{X^2-1}\right]$, they satisfy the identity

$$\left(X + \sqrt{X^2-1}\right)^n = T_n(X) + U_{n-1}(X)\sqrt{X^2-1}.$$

Hence (T_n, U_{n-1}) is a solution of the Pell's equation with $D(X) = X^2-1$, i.e.

$$T_n^2(X) - (X^2 - 1)U_{n-1}^2(X) = 1.$$

Theorem 1. *Let $P, Q, D \in \mathbb{C}[X]$ with $\deg(D) = 2$ and $\deg(P) = d$. The following conditions are equivalent:*

1. *P, Q, D satisfy the identity $P^2 - DQ^2 = 1$;*
2. *there are $\lambda, \mu \in \mathbb{C}^*$ and $\nu \in \mathbb{C}$ such that*

$$\begin{cases} P(X) = \pm T_d(\lambda X + \nu) \\ Q(X) = \mu U_{d-1}(\lambda X + \nu) \\ D(X) = \frac{(\lambda X+\nu)^2-1}{\mu^2}. \end{cases}$$

Remark 2. If d is odd, then T_d is an odd function and we can remove the sign $\pm$.

2 Parametric solutions

Now, we study the possible degrees of a parametric solution. We start giving an explicit description in the cases $\deg(P) = 1, 2$.

Proposition 3. *Let (a, b) be a solution of the Pell's equation (1) and let $P, Q, D \in \mathbb{Z}[X]$ with $\deg(D) = 2$ and $\deg(P) = 1$. Let*

$$c = \begin{cases} 1 & \text{if } b \text{ is odd} \\ 2 & \text{if } b \text{ is even.} \end{cases}$$

The following conditions are equivalent:

1. *P, Q, D satisfy*

$$\begin{cases} P^2 - DQ^2 = 1 \\ P(0) = a \\ Q(0) = b \\ D(0) = n; \end{cases}$$

2. *there is a nonzero integer m such that*

$$\begin{cases} P(X) = \frac{b^2 m}{c} X + a \\ Q(X) = b \\ D(X) = \frac{b^2 m^2}{c^2} X^2 + \frac{2am}{c} X + n. \end{cases}$$

Proposition 4. *Let (a, b) be a solution of the Pell's equation (1) and let $P, Q, D \in \mathbb{Z}[X]$ with $\deg(D) = 2$ and $\deg(P) = 2$. The following conditions are equivalent:*

1. *P, Q, D satisfy*

$$\begin{cases} P^2 - DQ^2 = 1 \\ P(0) = a \\ Q(0) = b \\ D(0) = n; \end{cases}$$

2. *there are two integers $m \neq 0$ and $\varepsilon \in \{\pm 1\}$ such that, if*

$$c = \gcd(b^3, (a + \varepsilon)b, 2(a + \varepsilon)^2),$$

then we have

$$\begin{cases} P(X) = \frac{b^4(a+\varepsilon)m}{c} X^2 + \frac{2b^2(a+\varepsilon)m}{c} X + a \\ Q(X) = \frac{b^3 m}{c} X + b \\ D(X) = \frac{b^2(a+\varepsilon)^2 m^2}{c^2} X^2 + \frac{2(a+\varepsilon)^2 m}{c} X + n. \end{cases}$$

Let n be a positive integer that is not a square and let $K = \mathbb{Q}(\sqrt{n})$ a quadratic real number field. Let O_K the ring of integers of K and let U the subgroup of $O_K^\times$ consisting of the units with norm 1. We have that U is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$. We also know that the elements of the subgroup $V = U \cap \mathbb{Z}[\sqrt{n}]$ correspond bijectively to the solutions of Pell's equation (1). We denote by $V(a, b)$ the subgroup of V generated by -1 and $a + b\sqrt{n}$. If (a, b) is a fundamental solution of Pell's equation (1) we have that $V(a, b) = V$. The quotient U/V is a finite cyclic group. The following theorem states that the degree of a parametric solution is bounded.

Theorem 5. *Let n be a positive integer that is not a square and let (a, b) a solution of Pell's equation (1). The following conditions are equivalent:*

1. *there is a parametric solution $P, Q, D \in \mathbb{Z}[X]$ of degree d associated to (a, b);*
2. *we have that $d \mid 2[U : V(a, b)]$.*

Without other assumptions on n this bound is not uniform, in fact for any positive integer d there are $a, b \in \mathbb{Z}$ such that

$$\left(2 + \sqrt{3}\right)^d = a + b\sqrt{3}.$$

Now, taking $n = 3b^2$ we have that $(a, 1)$ is a fundamental solution of $x^2 - ny^2 = 1$ and $d \mid [U : V(a, 1)]$. Hence, by Theorem 5 above, there is a parametric solution of degree d.

If we restrict to n squarefree, we have that if $n \equiv 2, 3 \pmod 4$ then U/V is trivial, else U/V is a subgroup of $\mathbb{Z}/3\mathbb{Z}$. Hence, d must divide 6. More precisely, if $n \equiv 2, 3 \pmod 4$ then $d = 1, 2$, else $d = 1, 2, 3, 6$.

References

[1] L. Zapponi, *Parametric solutions of Pell equations*, available at the URL `http://arxiv.org/abs/1503.00637`.

[2] *Parametric solutions of Pell's equations*, Discussion on the mathematical forum Mathoverflow, available at the URL `http://mathoverflow.net/questions/194910/`.

[3] *The Grothendieck theory of dessins d'enfants*, papers from the Conference on dessins d'enfant held in Luminy, April 1924, 1993. Edited by Leila Schneps. London Mathematical Society Lecture Note Series, **200**, Cambridge University Press, Cambridge, 1994.

Pietro Mercuri
Dipartimento di Matematica
Sapienza Università di Roma
Piazzale Aldo Moro 5
00185 Roma, Italy
email: mercuri.ptr@gmail.com

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 1, *Number* 1, *March* 2016, *pages* 49–57

Pieter Moree

Forbidden integer ratios of consecutive power sums

written by Cihan Pehlivan

1 Introduction

This is a report of the results obtained in joint work Pieter Moree (Bonn) and Ioulia Baoulina (Moscow), starting by providing background. For the details see [1].

For natural numbers $m, k \geqslant 1$ we consider the power sum

$$S_k(m) = 1^k + 2^k + \cdots + (m-1)^k.$$

For $k = 1, 2, 3$, $S_k(m)$ equals, respectively,

$$\frac{m(m-1)}{2}, \frac{(m-1)m(2m-1)}{6}, \frac{m^2(m-1)^2}{4}.$$

In the 17th century J. Faulhaber (1580-1635) realized that the power sums can be, in essence, expressed as polynomials in $S_1(m)$. Namely, there exists polynomials F_k and G_k such that

$$S_k(m) = \begin{cases} F_k(S_1(m)) \text{ with } \deg(F_k) = (k+1)/2 \text{ if } k \text{ is odd;} \\ S_2(m)G_k(S_1(m)) \text{ with } \deg(G_k) = (k-2)/2 \text{ if } k \text{ is even.} \end{cases}$$

The following theorem expresses the power sum $S_k(m)$ in terms of Bernoulli numbers B_k, which are defined by the identity

$$\frac{t}{e^t - 1} = \sum_{k=0}^{\infty} B_k \frac{t^k}{k!}.$$

Theorem 1 (Faulhaber) *For all positive integers m and k, we have*

$$S_k(m) = \frac{1}{k+1} \sum_{j=0}^{k} \binom{k+1}{j} B_j m^{k+1-j}.$$

E. Kummer in 1850 gave the following definition of an irregular prime.

Definition 2 *Write $B_k = \frac{u_k}{v_k}$ with $(u_k, v_k) = 1$. An odd prime p is called **irregular** if $p \mid u_k$ for some $k \in \{2, 4, \ldots, p-3\}$, and the pair (k, p) is called an **irregular pair**. An odd prime is called **regular** if it is not irregular.*

In 1851, Kummer obtained the following congruence, which plays an important role in the development of the theory of p-adic zeta functions.

Theorem 3 (Kummer) *If $\ell \equiv k \not\equiv 0 \pmod{p-1}$, then*

$$\frac{B_\ell}{\ell} \equiv \frac{B_k}{k} \pmod{p}.$$

Furthermore, he proved Fermat's Last Theorem for regular prime exponents.

Theorem 4 (Kummer) *If p is regular, then $x^p + y^p = z^p$ has only trivial solutions.*

In his work on Fermat's Last Theorem, Kummer also showed that p is regular when the class number $h_p = h(\mathbb{Q}(\zeta_p))$ of the pth cyclotomic field is not divisible by p.

Conjecture 5 (Kellner, 2011) *[3] Let m and k be positive integers with $m \geqslant 3$. Then the ratio*

$$\frac{S_k(m+1)}{S_k(m)} \text{ is an integer if and only if } (m,k) \in \{(3,1),(3,3)\}.$$

Hence, since $S_k(m+1) = S_k(m) + m^k$, we have

$$\frac{S_k(m+1)}{S_k(m)} \in \mathbb{Z} \quad \textit{iff} \quad \frac{m^k}{S_k(m)} \in \mathbb{Z}.$$

Kellner's conjecture is thus equivalent with the following one (in a moment we will see what Erdős and Moser have to do with it).

Conjecture 6 (Kellner–Erdős–Moser) *Let a, k, m be positive integers with $m \geqslant 3$. Then*

$$aS_k(m) = m^k \iff (a,k,m) \in \{(1,1,3),(3,3,3)\}.$$

In case $m = 3$ we have $aS_k(3) = 3^k$ and it follows that $a = 3^e$ for some $e \geq 0$. Then $1 + 2^k = 3^{k-e}$, which has as only solutions $1 + 2 = 3$ and $1 + 2^3 = 3^2$ (as was already known in the Middle Ages).

In case $a = 1$, we obtain the following special case of the Kellner-Erdős-Moser conjecture.

Conjecture 7 (Erdős, 1950) *The Diophantine equation*

$$1^k + 2^k + \cdots + (m-1)^k = m^k \tag{1}$$

has only one solution, namely $1 + 2 = 3$.

A few years after Erdős made his conjecture L. Moser proved the following theorem.

Theorem 8 (Moser, 1953) *[7], cf. [4] If (m,k) is a solution of* (1) *with $k \geqslant 2$, then $m > 10^{10^6}$.*

The lower bound for m can be sharpened to $m > 10^{9\cdot 10^6}$, see P. Moree [4]. In 2011, Y. Gallot, P. Moree and W. Zudilin [2] using completely different methods again sharpened the lower bound.

Theorem 9 *[2] If (m, k) is a solution of (1) with $k \geqslant 2$, then $m > 10^{10^9}$.*

For the general case $aS_k(m) = m^k$, in 2015, I. Baoulina and P. Moree [1] established the following results.

Theorem 10 *If $aS_k(m) = m^k$ with $m > 3$, then*

- *a has no regular prime divisors;*
- *$a = 1$ or $a > 1500$;*
- *m has no regular prime divisors;*
- *$k, m > 10^{82}$;*
- *$k, m > 10^{9\cdot 10^6}$ if $m \equiv 1 \pmod 3$;*
- *$k, m > 10^{4\cdot 10^{20}}$ if $m \equiv 1 \pmod{30}$.*

Theorem 11 *Suppose that (m, k) is a non-trivial solution of $aS_k(m) = m^k$ and p is a prime dividing m. Then*

- *p is an irregular prime;*
- *$p^2 \mid u_k$;*
- *$k \equiv r \pmod{p-1}$ for some irregular pair (r, p).*

In case $a = 1$ this result is due to P. Moree, H. te Riele and J. Urbanowicz [6].

Corollary 12 *If a has a regular prime divisor, then the equation*

$$aS_k(m) = m^k$$

has only trivial solutions.

In 1915, K. L. Jensen proved the following theorem.

Theorem 13 *There are infinitely many primes $p \equiv 5 \pmod 6$ that are irregular.*

Note that it is still not known whether there are infinitely many regular primes. Let us define

$$\pi_i(x) := \#\{p \leqslant x : p \text{ is irregular}\}.$$

In 1954, C. L. Siegel provided an heuristic argument to justify the conjecture that

$$\pi_i(x) \sim \left(1 - \frac{1}{\sqrt{e}}\right)\pi(x) \sim 0.39...\frac{x}{\log x}.$$

We will make the following weaker conjecture.

Conjecture 14 *There exists $\delta \in (0, 1)$ such that*

$$\pi_i(x) < (1 - \delta)\frac{x}{\log x} \text{ as } x \to \infty.$$

Let I be the set of integers composed solely of irregular primes. Suppose that conjecture (14) holds true. The standard theory of the average behaviour of arithmetical functions yields that $I(x) \ll x(\log x)^{-\delta}$. On combining this estimate and Corollary 12 we then obtain the following result.

Proposition 15 *Under Conjecture 14 the set of integer ratios that are of the form $S_k(m + 1)/S_k(m)$ with $m \geq 3$ has zero natural density.*

We now briefly consider how to deal with $aS_k(m) = m^k$ for a prescribed a.

A pair $(t, q)_a$ with q a prime and $2 \leqslant t \leqslant q-3$ even is called **helpful** if $q \nmid a$ and, for every $c = 1, 2, \ldots, q - 1$, we have

$$aS_t(c) \not\equiv c^t \pmod q.$$

If q is an irregular prime, we require in addition that (t, q) should not be an irregular pair.

Lemma 16 *[1] If $(t, q)_a$ is a helpful pair and (m, k) a solution of*

$$aS_k(m) = m^k$$

with k even, then $k \not\equiv t \pmod{q-1}$.

Suppose that $1 < a \leqslant 1500$. Then the equation $aS_k(m) = m^k$ has no non-trivial solutions except possibly when a is an irregular prime or $a = 37 \times 37$. We have $\pi(1500) = 239$, $\pi_i(1500) = 90$ and $\frac{90}{239} \approx 0.38$.

Example 17 *Consider $673S_k(m) = m^k$; $(408, 673)$, $(502, 673)$ are the irregular pairs.*
Reduction modulo 5:

- $3S_k(m) \equiv m^k \pmod 5$
- $k \equiv 502 \pmod{672} \subset k \equiv 2 \pmod 4$
- $(2, 5)_3$ *is helpful*

Reduction modulo 17:

- $10S_k(m) \equiv m^k \pmod{17}$
- $k \equiv 408 \pmod{672} \subset k \equiv 8 \pmod{16}$
- $(8, 17)_{10}$ *is helpful*

So, the equation has no solutions.

2 Start of Moser's proof of Theorem 8

Consider a prime p so that m^k takes a simple form modulo p. The most obvious choice is to take p to be a prime divisor of $m-1$. On using that the power sum as a function of k is periodic modulo p, the equation (1) reduces to

$$S_k(m) \equiv \frac{m-1}{p}\,(1^k + 2^k + \cdots + (p-1)^k) \equiv m^k \equiv 1 \pmod p. \quad (2)$$

Proposition 18 *[4] Let $p \mid m-1$ be a prime. Modulo p we have*

$$S_k(p) \equiv \begin{cases} -1 & \text{if } p-1 \text{ divides } k; \\ 0 & \text{otherwise.} \end{cases}$$

By the proposition we have $S_k(p) \equiv -1 \pmod{p}$, and hence by (2) we must have

$$\frac{m-1}{p} + 1 \equiv 0 \pmod{p}.$$

We conclude that $m-1$ must be squarefree and hence that

$$\prod_{p \mid m-1} \left(\frac{m-1}{p} + 1 \right) \equiv 0 \pmod{m-1},$$

On expanding the product we obtain

$$\prod_{p \mid m-1} \left(\frac{m-1}{p} + 1 \right) = 1 + \sum_{p \mid m-1} \frac{m-1}{p} + \sum_{\substack{p_1, p_2 \mid m-1 \\ p_1 \neq p_2}} \frac{(m-1)^2}{p_1 p_2} + \cdots,$$

where the sum involving the primes p_1, p_2 and the sums not indicated involving three primes or more are divisible by $m-1$. Hence we obtain

$$\sum_{p \mid m-1} \frac{m-1}{p} + 1 \equiv 0 \pmod{m-1},$$

which on division by $m-1$ gives

$$\sum_{p \mid m-1} \frac{1}{p} + \frac{1}{m-1} \in \mathbb{Z}_{\geqslant 1}. \tag{3}$$

Writing the equation $S_k(m) = m^k$ as $S_k(m+2) = 2m^k + (m+1)^k$ and using the proposition, we get

$$\sum_{p \mid m+1} \frac{1}{p} + \frac{2}{m+1} \in \mathbb{Z}_{\geqslant 1}. \tag{4}$$

By similar ad hoc arguments one is led to the following two conclusions:

$$\sum_{p\,|\,2m-1} \frac{1}{p} + \frac{2}{2m-1} \in \mathbb{Z}_{\geqslant 1}; \tag{5}$$

$$\sum_{p\,|\,2m+1} \frac{1}{p} + \frac{4}{2m+1} \in \mathbb{Z}_{\geqslant 1}. \tag{6}$$

On adding the four equations (3), (4), (5) and (6), we obtain

$$\sum_{p\,|\,M} \frac{1}{p} + \frac{1}{m-1} + \frac{2}{m+1} + \frac{2}{2m-1} + \frac{4}{2m+1} \geqslant 3\frac{1}{6},$$

where $M = (m^2-1)(4m^2-1)/12$. Using the fact that $\sum_{p\leqslant 10^7} \frac{1}{p} < 3.16$, we find $M > \prod_{p\leqslant 10^7} p$. This gives $m > 10^{10^6}$.

Details of the proof can be found in P. Moree [4] and L. Moser [7]. The title of [4] refers to the four, in an ad hoc way derived, equations (3), (4), (5) and (6) ("the four mathemagical rabbits") and the fact that they can be actually obtained from one theorem ("the top hat").

For a survey of work on the Erdős-Moser equation the reader can consult [5].

3 Challenges

- Can one use that $p^2 \mid u_k$ (with $p \mid a$), rather than $p \mid u_k$?
- Show that Conjecture 7 implies Conjecture 6.
- Write a program to deal with $aS_k(m) = m^k$ for a given a.
- Show that if $S_k(m) = bm^k$, then $120 \mid k$.
- Study the equation $aS_k(m) = bm^k$.

References

[1] I. Baoulina and P. Moree, *Forbidden integer ratios of consecutive power sums,* In: *From Arithmetic to Zeta-Functions – Number Theory in Memory of Wolfgang Schwarz*, Springer, Basel (to appear), http://arxiv.org/abs/1510.06064.

[2] Y. Gallot, P. Moree, and W. Zudilin, *The Erdős–Moser equation* $1^k + 2^k + \cdots + (m-1)^k = m^k$ *revisited using continued fractions*, Math. Comp. **80** (2011), 1221-1237.

[3] B. C. Kellner, *On stronger conjectures that imply the Erdős-Moser conjecture,* J. Number Theory **131** (2011), 1054-1061.

[4] P. Moree, *A top hat for Moser's four mathemagical rabbits,* Amer. Math. Monthly **118** (2011), 364–370.

[5] P. Moree, *Moser's mathemagical work on the equation* $1^k + 2^k + \ldots + (m-1)^k = m^k$*,* Rocky Mountain J. of Math. **43** (2013), 1707-1737.

[6] P. Moree, H. te Riele, and J. Urbanowicz, *Divisibility properties of integers* x, k *satisfying* $1^k + \cdots + (x-1)^k = x^k$*,* Math. Comp. **63** (1994), 799-815.

[7] L. Moser, *On the diophantine equation* $1^n+2^n+3^n+\cdots+(m-1)^n = m^n$*,* Scripta Math. **29** (1953) 84-88.

Cihan Pehlivan
Dipartimento di Matematica e Fisica
Università Roma Tre
Largo San Leonardo Murialdo 1
00146 Rome, Italy
email: cihanp@gmail.com

PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 1, *Number* 1, *March* 2016, *pages* 59–66

Joël Rivat

Digital properties of prime numbers

written by Claudio Stirpe

1 Introduction

This exposition deals with the digits of prime numbers and oulines some recent results in a joint work of Joël Rivat and Christian Mauduit.

Some of the typical questions that mathematicians are likely to think about include:

- "Are prime number random?"
- "What type of results to expect?"

This is an introduction to some ideas focusing on what kind of result one may expect.

2 Prime Number Theorem and Möbius Random Principle

Let p be a prime and consider the von Mangoldt function defined as

$$\Lambda(n) = \log p$$

for $n = p^k$ and zero otherwise.

The famous *Prime Number Theorem* due to Hadamard [1] and, independently, to de la Vallée Poussin [2] states that

$$\sum_{n \le x} \Lambda(n) = x + o(x). \tag{1}$$

Let f be a function defined over the natural numbers. We say that f satisfies Prime Number Theorem (PNT) if $\sum_{n \le x} \Lambda(n) f(n)$ admits an asymptotic formula.

The special case when $f(n) = \exp(2\pi i \alpha n)$ is relevant for Vinogradov 3-primes Theorem [13]: *Let*

$$r(N) = \sum_{k_1+k_2+k_3=N} \Lambda(k_1)\Lambda(k_2)\Lambda(k_3).$$

Then

$$r(N) = \frac{1}{2} \prod_{p \mid N} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{p \nmid N} \left(1 + \frac{1}{(p-1)^3}\right) N^2 + O\left(\frac{N^2}{\log^A N}\right) \tag{2}$$

where A is a fixed positive real number. The proof of (2) is based on the identity:

$$r(N) = \int_0^1 \left(\sum_{n=1}^{N} \Lambda(n) \exp(2\pi i \alpha n)\right)^3 \exp(-2\pi i \alpha N)\, d\alpha.$$

Vinogradov's result implies that every sufficiently large odd integer n can be written as the sum of three primes. The result was extended by Helfgott [8] to all $n \ge 5$.

An other natural question is "Has n an odd number of primes in its factorization or not?". This is the reason why Möbius function arises as

$$\mu(n) = (-1)^k,$$

where k is the number of distinct primes dividing n for any squarefree n and $\mu(n) = 0$ otherwise.

As above we say that f satisfies Möbius Random Principle (MRP) if $\sum_{n\leq x}\mu(n)f(n)$ is close to zero.

These concepts are strongly related with Sarnak's conjecture [12] which relies on determining types of prime densities and functions produced by zero topological entropy dynamical system.

MRP is easy to prove for $f = 1$ as $\sum_{n\leq x}\mu(n) = o(x)$. The reader may compare this result with (1) which states that $f = 1$ satisfies PNT, but MRP is sometimes easier to show than PNT for general f.

3 Are prime number digits random?

Now we turn to prime numbers. Are the digits of prime numbers random? This is a difficult question so we formulate it into another way using Gelfond's results [7]. Let $q \geq 2$ be an integer and let $\epsilon_j(n)$ be the j-th digit in the q-ary expansion of n and consider

$$S(n) = \sum_j \epsilon_j(n).$$

We recall a property of $S(n)$ about arithmetic progressions $\{s+km|\ k \in \mathbb{Z}\}$.

Theorem 1 (Gelfond [7], 1968) *Given an integer $m \geq 2$, prime to $q-1$, there exists $\sigma_m > 0$ such that for any integer $m' > 0$ and for any arithmetic progression $A = \{s+km|\ k \in \mathbb{Z}\}$ and $A' = \{s'+km'|\ k \in \mathbb{Z}\}$*

$$\sum_{n\leq x,\ (S(n),n)\in(A,A')} 1 = \frac{x}{m'm} + O(x^{1-\sigma_m}).$$

Again compare this formula with (1). The sum of digits is well distributed in arithmetic progressions !

Gelfond underlines two important problems:

1. Evaluate the number of prime numbers $p \leq x$ such that $S(p) \equiv a \mod m$;

2. Consider polynomial analogues: evaluate the number of integers $n \leq x$ such that $S(P(n)) \equiv a \mod m$, where P is a polynomial.

In the rest of this note, we will focus on the first question only.

In 2010, for $f(n) = \exp(2\pi i \alpha S(n))$ and α satisfing $(q-1)\alpha \in \mathbb{R} - \mathbb{Z}$, a PNT properties was estabilished in [10]. Namely

$$\left| \sum_{n \leq x} \Lambda(n) \exp(2\pi i \alpha S(n)) \right| \leq C_q(\alpha) x^{1-\sigma_q(\alpha)},$$

for suitable constants $C_q(\alpha)$ and $\sigma_q(\alpha)$ depending on q and α.

Let $(p_n)_{n\geq 1}$ denote the sequence of prime numbers. By the previous result, the sequence $(\alpha S(p_n))_{n\geq 1}$ is equidistributed modulo 1 for any $\alpha \in \mathbb{R} - \mathbb{Z}$. Moreover for any integer a and $m \geq 2$, with m prime to $q-1$ we get

$$\sum_{\substack{p \leq x \\ S(p) \equiv a \mod m}} 1 \sim \frac{1}{m} \sum_{p \leq x} 1,$$

for large x.

In 2005 Dartyge-Tenenbaum [4] proved a similar result for MRP.

A more difficult result [5] was obtained in 2009 about the number of primes p satisfing $S(p) = k$. This number is close to the expected value $\frac{q-1}{2} \log_q x$ as follows:

$$|\{p \leq x |\ S(p) = k\}| =$$

$$\frac{(q-1)\pi(x)}{\varphi(q-1)\sqrt{2\pi\sigma_q^2 \log_q x}} \exp\left(\frac{-(k - \mu_q \log_q x)^2}{2\sigma_q^2 \log_q x}\right) + O((\log_q x)^{-\frac{1}{2}+\epsilon}),$$

where we denote by μ_q and σ_q the numbers $\frac{q-1}{2}$ and $\frac{q^2-1}{12}$, respectively. and $\epsilon > 0$ is an arbitrary, fixed real number. Such a local result was previously considered "hopelessly difficult" by Erdös!

One may also fix digits and their positions and wonder about asymptotic properties only. Recently, in 2014, Bourgain showed the existence

of an asymptotical formula for the existence of a small constant $c > 0$ such that for given integers k and ℓ with $1 \le \ell \le ck$ we get

$$\left|\{p < 2^k, \epsilon_{j_1}(p) = b_1, \ldots, \epsilon_{j_\ell}(p) = b_\ell\}\right| \sim \frac{1}{2^\ell}\frac{2^k}{\log 2^k},$$

for large k, and for any choise of $1 < j_1 < \ldots < j_\ell = k - 1$ and $(b_1, \ldots, b_\ell) \in \{0, 1\}^\ell$ with $b_\ell = 1$.

We can also consider more general functions f and try to establish similar properties: similar results are given for strongly q-multiplicative functions f (see [9]) and for block counting functions, as Rudin-Shapiro sequence, see the following section.

4 Correlations in the Rudin–Shapiro sequence

We need new ideas for handling sequences like $111\ldots111$. Such sequences arises in Mersenne primes $2^n - 1$. So in this section we study correlations of digits.

Let δ be a positive integer. We define

$$\beta_\delta(n) = \sum_k \epsilon_{k-\delta-1}(n)\epsilon_k(n).$$

This is the number of pairs of 1 in the representation of n with given distance $\delta + 1$. A recent result [11] states that for any real α and θ there exists explicit constants $C(\delta)$ and $\sigma(\alpha) > 0$ such that

$$\left|\sum_{n\le x} \Lambda(n)\exp(\beta_\delta(n)\alpha + \theta n)\right| \le C(\delta)(\log x)^{\frac{11}{4}} x^{1-\sigma(\alpha)}$$

and

$$\left|\sum_{n\le x} \mu(n)\exp(\beta_\delta(n)\alpha + \theta n)\right| \le C(\delta)(\log x)^{\frac{11}{4}} x^{1-\sigma(\alpha)}.$$

A second generalization about blocks of d consecutive 1's gives very similar results.

Remark 2 *Our approach can be summarized in a few steps:*

1. *A first step is reducing the problem to an exponential sum.*
2. *Then we remove some digits, namely the upper range and the lower range, using Van der Corput's inequality, and this leads to focus on the digits in the middle range only.*
3. *Separating the problem in two parts is also useful: a discrete part and an analytical part.*
4. *For the first part we may use discrete Fourier transform. For the second we use analytic methods to see which Fourier estimates are needed. We may study the lowest terms of the string by passing n modulo any integer l. We may also consider the first digits by dividing with powers of q.*
5. *Finally, obtain the corresponding Fourier estimates.*

5 Open problems

We finish this overview with three open problems.

1. What about the digits of p^2?

   This problem is completely open and not so easy to handle.

2. Consider the sequence $(t_{P(p_n)})_{n\in\mathbb{N}}$, where $t_n = (-1)^{S(n)}$ is the Thue-Morse sequence and P is a non constant polynomial with $P(n) \in \mathbb{N}$ for any $n \in \mathbb{N}$. Is it true that this sequence is normal?

3. What can we say from a dynamical system point of view?

References

[1] J. Hadamard, *Sur la distribution des zéros de la fonction $\zeta(s)$ et ses conséquences arithmétiques*, Bull. Soc. Math. France **24**, 199–220 (1896).

[2] Ch.-J. de la Vallée Poussin, *Recherches analytiques sur la théorie des nombres premiers*, Brux. S. sc. **21**, 183–256, 281–362, 363–397 (1896).

[3] J. Bourgain, *Prescribing the binary digits of primes*, Israel J. Math. **194**, no. 2, 935–955 (2013).

[4] C. Dartyge, and G. Tenenbaum, *Sommes des chiffres de multiples d'entiers*, Ann. Inst. Fourier (Grenoble) **55**, 2423–2474 (2005).

[5] M. Drmota, C. Mauduit, and J. Rivat, *Primes with an average sum of digits*, Compos. Math. **145**, no. 2, 271–292 (2009).

[6] M. Drmota, C. Mauduit, and J. Rivat, *The sum-of-digits function of polynomial sequences*. J. Lond. Math. Soc. (2), **84**, 81–102 (2011).

[7] A. O. Gelfond, *Sur les nombres qui ont des propriétés additives et multiplicatives données*, Acta Arithmetica **13**, 259–265 (1968).

[8] H. A. Helfgott, *The ternary Goldbach problem*, `arXiv:1501.05438v2 [math.NT]`.

[9] B. Martin, M. Mauduit, and J. Rivat, *Prime Number Theorem for digital functions*, Acta Arith. **165**, no. 1, 11–45 (2014).

[10] C. Mauduit, and J. Rivat, *Sur un problème de Gelfond: la somme des chiffres des nombres premiers*, Ann. of Math. (2) **171**, no. 3, 1591–1646 (2010).

[11] C. Mauduit, and J. Rivat, *Prime numbers along Rudin–Shapiro sequences*, J. Eur. Math. Soc. **27**, 2595–2642 (2015).

[12] P. Sarnak, *Mobius randomness and dynamics*, lecture slides summer 2010 http://www.math.princeton.edu/sarnak/.

[13] I. M. Vinogradov, *The method of Trigonometrical Sums in the Theory of Numbers, translated from the Russian, revised and annotated by K. F. Roth and A. Davenport*, Interscience, London 1954.

Claudio Stirpe
Dipartimento di Matematica
Sapienza Università di Roma
Piazzale Aldo Moro 5
I–00185 Rome, ITALY
email: stirpe@mat.uniroma1.it