Alessandro Languasco: Abstracts of Publications

November 20, 2021

My scientific ID-codes are : Orcid ID; Scopus Author ID; Thomson Reuters Researcher ID; Researchgate page; Google Scholar profile, Mathematical Reviews.

Books

[1] A. Languasco. *Analisi Matematica 1*. Ulrico Hoepli editore, 2017. http://www.hoepli.it/libro/analisi-matematica-1/9788820380823.html.

Abstract: Dopo una esperienza ventennale di insegnamento su corsi universitari di analisi matematica, ho deciso di organizzare parte del materiale sviluppato in questi anni nel presente testo. L'esigenza è nata dal fatto che, a seguito delle ultime riforme universitarie e della contrazione dell'orario di insegnamento dei corsi di analisi matematica, si è poco a poco preferito una presentazione degli argomenti classici del calcolo differenziale e integrale che privilegia il "saper fare" e una didattica sempre più votata far prevalere le modalità di presentazione a scapito del rigore dei contenuti. Di conseguenza, l'aspetto relativo a una comprensione completa e rigorosa di tali concetti ha perso spazio e importanza. Ritenendo, al contrario, che per poter usare uno strumento matematico sia assolutamente necessario avere compreso *in quali casi* e *sotto quali condizioni* sia possibile adoperarlo, penso che lo scopo principale dei corsi universitari di matematica sia, oggi più che mai, quello di educare all'utilizzo del procedimento *logico-deduttivo*. In tal modo si permetterà agli studenti di cominciare a maturare una disciplina mentale - lo strumento di investigazione principale di chiunque si occupi di scienza - che si rivelerà non solo essere vincente per superare l'esame finale del corso, ma consentirà loro di affrontare con competenza le variegate applicazioni della matematica che incontreranno nella successiva carriera. In questo testo ho quindi mantenuto al minimo la quantità di informazioni date come "intuitive" limitandole, essenzialmente, alla *teoria degli insiemi*, a qualche aspetto della costruzione degli insiemi numerici fondamentali e ad alcune proprietà delle funzioni trigonometriche; e ho poi inserito una trattazione dettagliata e rigorosa, ma elementare, di tutti i classici argomenti del calcolo differenziale e integrale per funzioni di una variabile reale. In particolare ho mostrato, senza "saltare" dimostrazioni o semplificare eccessivamente la trattazione introducendo ipotesi non necessarie, la *teoria dei limiti* e il *calcolo differenziale e integrale* per funzioni di una variabile reale, le *successioni* e le *serie numeriche*, le *serie di potenze* e alcuni cenni alla *teoria delle equazioni differenziali ordinarie*. Ho evitato di addentrarmi nella *teoria della cardinalità*, che usualmente viene affrontata nel primo corso di algebra del corso di laurea in matematica, o di presentare concetti quali la *compattezza* o la *completezza* perché ritengo che essi possano essere introdotti solo a studenti con maggiore esperienza. Per lo stesso motivo ho presentato la *teoria dell'integrazione* secondo Riemann e non quella, più sofisticata, di Lebesgue. Per quanto riguarda la trattazione delle *equazioni differenziali ordinarie*, mi sono limitato a esporre solamente i casi più semplici perché una presentazione più completa richiede la conoscenza del calcolo differenziale per funzioni di più variabili reali; un argomento tipico di un secondo corso di analisi matematica. Per la stessa ragione, ho trattato le *serie di potenze* senza introdurre il concetto più generale di *serie di funzioni*. Nei complementi ho raccolto alcuni argomenti affrontabili con gli strumenti presentati nel testo ma che non fanno usualmente parte del programma. Dato che la quantità di materiale esposta di seguito è di certo troppo ampia per poter essere del tutto inserita in un primo corso di analisi matematica, il docente dovrà decidere dove operare le opportune "scorciatoie"; ma lo studente che ha bisogno di maggiori dettagli per meglio comprendere tali tematiche potrà qui trovare una trattazione completa anche degli argomenti non presentati a lezione. In tal modo il testo può essere usato per un primo corso rivolto a studenti dei corsi di laurea in matematica, in fisica, in ingegneria e in informatica. Infine, affinché gli studenti possano impadronirsi del *calcolo*, ossia dell'uso "pratico" degli strumenti matematici qui introdotti, ho inserito nel testo anche vari esempi ed esercizi svolti, e diversi altri tipi di esercizi sono presentati al fondo di ogni capitolo. Alcune risoluzioni di questi ultimi sono presentati all'indirizzo **www.hoeplieditore.it/8082-3** in cui verranno anche inseriti eventuali complementi alla trattazione.

[2] A. Languasco and A. Zaccagnini. *Manuale di Crittografia*. Ulrico Hoepli Editore, 2015. http://www.hoepli.it/libro/manuale-di-crittografia/9788820366902.html.

Abstract: Fin dall'antichità si sono ideati metodi sempre più sicuri per occultare il reale significato di determinati segni e rendere un messaggio "offuscato", in modo che non sia comprensibile a persone non autorizzate a leggerlo. Obiettivo di questo volume è presentare il linguaggio della crittografia moderna e dei vari aspetti collegati. Dopo un'introduzione storica che consente di acquisire dimestichezza con la terminologia e i problemi della disciplina, il testo tratta alcuni sistemi crittografici simmetrici (DES, AES) e asimmetrici. In particolare sono descritti gli algoritmi necessari per comprendere e implementare i crittosistemi e alcuni dei protocolli crittografici oggi più utilizzati. Vengono inoltre illustrati gli aspetti fondamentali della crittografia probabilistica. La completezza della trattazione che illustra tutti gli aspetti coinvolti (storia, matematica, algoritmi, applicazioni, complessità computazionale) rende questo volume adatto non solo agli studenti universitari di Informatica, Matematica e

Ingegneria Informatica, ma anche a chiunque sia interessato a conoscere il linguaggio della crittografia moderna. L'intero testo è integrato da numerosi esempi, diagrammi e figure, mentre materiali di complemento, tra cui diversi esempi "pratici" (svolti utilizzando il software Pari/Gp) sono disponibili online.

[3] A. Languasco and A. Zaccagnini. *Crittografia*. CLEUP, Padova, 2006. Progetto Lauree Scientifiche per il Veneto.

Abstract: Queste sono le note del materiale preparato per lo svolgimento degli Incontri del Progetto Nazionale Lauree Scientifiche per il Veneto, sottoprogetto Matematica, per la tematica Crittografia.

[4] A. Languasco and A. Zaccagnini. *Introduzione alla Crittografia*. Ulrico Hoepli Editore, 2004.

Abstract: Lo scopo primario degli autori è la presentazione del linguaggio della Crittografia moderna e dei suoi problemi. Il libro fornisce la base matematica che permette di comprenderne il funzionamento, al fine di consentire un utilizzo più consapevole degli strumenti crittografici anche a chi non ha intenzione di diventare un professionista del campo. Vengono presentati alcuni sistemi crittografici simmetrici (DES, AES) ed asimmetrici (fra i quali il popolare RSA), la cui sicurezza è basata sulla presunta difficoltà dei problemi della fattorizzazione dei numeri interi e del logaritmo discreto. In particolare sono analizzati gli attacchi noti a RSA ed alcune precauzioni implementative, sono trattati gli algoritmi necessari per implementare i crittosistemi e sono descritti alcuni Protocolli crittografici utilizzati al giorno d'oggi. Inoltre è introdotto uno strumento specifico per calcoli teorico-numerici (PARI/Gp). Arricchiscono questo volume numerosi esempi, diagrammi e figure che lo rendono accessibile a qualunque lettore.

IN PREPARATION

[5] A. Languasco, P. Moree, S. Saad Eddin, and A. Sedunova. Computation of the Kummer ratio of the class number for prime cyclotomic fields. *Arxiv*, 2019. http://arxiv.org/abs/1908.01152v3.

Abstract: Let ζ_q be a primitive q^{th} root of unity with q an arbitrary odd prime. The ratio of Kummer's first factor of the class number of the cyclotomic number field $\mathbb{Q}(\zeta_q)$ and its expected order of magnitude (a simple function of q) is called the Kummer ratio and denoted by $r(q)$. It is known that typically $r(q)$ is close to 1, but nevertheless it is believed that it is unbounded, but only large on a very thin sequence of primes q. We propose an algorithm to compute $r(q)$ requiring the evaluation of $\mathcal{O}(q \log q)$ products and $\mathcal{O}(q)$ logarithms. Using it we obtain a new record maximum for $r(q)$, namely $r(6766811) = 1.709379\ldots$ (the old record being $r(5231) = 1.556562\ldots$) and a new record minimum, namely $r(116827429) = 0.575674\ldots$ (the old record being $r(3) = 0.604599\ldots$). The program used and the results described here, are collected at the address http://www.math.unipd.it/~languasc/rq-comput.html. This is a (preliminary) report about the computational part of a joint project with Pieter Moree, Sumaia Saad Eddin and Alisa Sedunova.

[6] A. Languasco and M. Migliardi. Efficient computation of the Dirichlet-multinomial log-likelihood function and applications. 2020. http://dx.doi.org/10.13140/RG.2.2.32923.28962.

Abstract: We introduce a new algorithm to compute the main quantity required in the Dirichlet-multinomial log-likelihood function, i.e., using notations in literature, $\log\Gamma(1/x + y) - \log\Gamma(1/x)$, where $x > 0$, $y \in \mathbb{N}$, $y \geq 1$, and Γ is Euler's function. Such an algorithm has the same stability for $x \to 0^+$ than Yu-Shaw's mesh method but it has a much better computational complexity and a wider range of application. In particular, our result works under the condition $x < 1$ which is weaker than $xy < 1$ needed in Yu-Shaw's method; thus removing the necessity of building a mesh of points.

PREPRINTS

[7] A. Ciolan, A. Languasco, and P. Moree. Landau and Ramanujan approximations for divisor sums and coefficients of cusp forms. *ArXiv*, 2021. http://arxiv.org/abs/2109.03288, submitted.

Abstract: In 1961, Rankin determined the asymptotic behavior of the number $S_{k,q}(x)$ of positive integers $n \leq x$ for which a given prime q does not divide $\sigma_k(n)$, the k-th divisor sum function. By computing the associated Euler-Kronecker constant $\gamma_{k,q}$, which depends on the arithmetic of certain subfields of $\mathbb{Q}(\zeta_q)$, we obtain the second order term in the asymptotic expansion of $S_{k,q}(x)$. Using a method developed by Ford, Luca and Moree (2014), we determine the pairs (k, q) with $(k, q-1) = 1$ for which Ramanujan's approximation to $S_{k,q}(x)$ is better than Landau's. This entails checking whether $\gamma_{k,q} < 1/2$ or not, and requires a substantial computational number theoretic input and extensive computer usage. We apply our results to study the non-divisibility of Fourier coefficients of six cusp forms by certain exceptional primes, extending the earlier work of Moree (2004), who disproved several claims made by Ramanujan on the non-divisibility of the Ramanujan tau function by five such exceptional primes.

[8] A. Languasco. Efficient computation of some special functions. *Arxiv*, 2021. http://arxiv.org/abs/2111.07686.

Abstract: We introduce a new algorithm to efficiently compute the functions belonging to a suitable set $\mathcal{F}$ defined as follows: $f \in \mathcal{F}$ means that $f(s,x)$, $s \in A \subset \mathbb{R}$ being fixed and $x > 0$, has a power series expansion centred at $x_0 = 1$ and satisfies a difference equation of step 1; moreover, we will also require that the Euler-Maclaurin summation formula can be applied to f. Denoting Euler's function as Γ, we will show, for $x > 0$, that $\log\Gamma(x)$, the digamma function $\psi(x)$, the polygamma functions $\psi^{(w)}(x)$, $w \in \mathbb{N}$, $w \geq 1$, and, for $s > 1$ being fixed, the Hurwitz $\zeta(s,x)$-function and its first partial derivative $\frac{\partial\zeta}{\partial s}(s,x)$ are in $\mathcal{F}$. In all these cases the coefficients of the involved power series will depend on the values of $\zeta(u)$, $u > 1$, where ζ is Riemann's function. As a by product, we will also show how to compute efficiently the Dirichlet L-functions $L(s,\chi)$ and $L'(s,\chi)$, $s > 1$, χ being a primitive Dirichlet character, by inserting the reflection formulae of $\zeta(s,x)$ and $\frac{\partial\zeta}{\partial s}(s,x)$ into the first step of the Fast Fourier Transform algorithm. Moreover, we will obtain some new formulae and algorithms for the Dirichlet β-function and for the Catalan constant G. Finally, we will study the case of the Bateman G-function. In the last section we will also describe some tests that show an important performance gain with respect to a standard multiprecision implementation of $\zeta(s,x)$ and $\frac{\partial\zeta}{\partial s}(s,x)$, $s > 1$, $x > 0$.

To Appear

[9] Y. Lamzouri and A. Languasco. Small values of $|L'/L(1,\chi)|$. *Experimental Mathematics,* electronically published on September 3, 2021, DOI:https://doi.org/10.1080/10586458.2021.1927255 (to appear in print), 2021. MR:, ZBL:.

Abstract: In this paper, we investigate the quantity $m_q := \min_{\chi\neq\chi_0} |L'/L(1,\chi)|$, as $q \to \infty$ over the primes, where $L(s,\chi)$ is the Dirichlet L-function attached to a non trivial Dirichlet character modulo q. Our main result shows that $m_q \ll \log\log q/\sqrt{\log q}$. We also compute m_q for every odd prime q up to 10^7. As a consequence we numerically verified that for every odd prime q, $3 \leq q \leq 10^7$, we have $c_1/q < m_q < 5/\sqrt{q}$, with $c_1 = 21/200$. In particular, this shows that $L'(1,\chi) \neq 0$ for every non trivial Dirichlet character χ mod q where $3 \leq q \leq 10^7$ is prime, answering a question of Gun, Murty and Rath in this range. We also provide some statistics and scatter plots regarding the m_q-values, see Section 6. The programs used and the computational results described here are available at the following web address: http://www.math.unipd.it/~languasc/smallvalues.html.

[10] A. Languasco and T.S. Trudgian. Uniform effective estimates for $|L(1,\chi)|$. *Journal of Number Theory,* electronically published on August 24, 2021, DOI:https://doi.org/10.1016/j.jnt.2021.07.019 (to appear in print), 2022. MR:, ZBL:.

Abstract: Let $L(s,\chi)$ be the Dirichlet L-function associated to a non-principal primitive Dirichlet character χ defined mod q, where $q \geq 3$. We prove, under the assumption of the Generalised Riemann Hypothesis, the validity of estimates given by Lamzouri, Li, and Soundararajan on $|L(1,\chi)|$. As a corollary, we have that similar estimates hold for the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-q})$, $q \geq 5$.

Published Papers (in reverse chronological order)

[11] A. Languasco. Efficient computation of the Euler-Kronecker constants for prime cyclotomic fields. *Research in Number Theory*, 7:1–22, 2021. http://dx.doi.org/10.1007/s40993-020-00213-1, MR:4194178, ZBL:07304549.

Abstract: We introduce a new algorithm, which is faster and requires less computing resources than the ones previously known, to compute the Euler-Kronecker constants $\mathfrak{G}_q$ for the prime cyclotomic fields $\mathbb{Q}(\zeta_q)$, where q is an odd prime and ζ_q is a primitive q-root of unity. With such a new algorithm we evaluated $\mathfrak{G}_q$ and $\mathfrak{G}_q^+$, where $\mathfrak{G}_q^+$ is the Euler-Kronecker constant of the maximal real subfield of $\mathbb{Q}(\zeta_q)$, for some very large primes q thus obtaining two new negative values of $\mathfrak{G}_q$: $\mathfrak{G}_{9109334831} = -0.248739\ldots$ and $\mathfrak{G}_{9854964401} = -0.096465\ldots$ We also evaluated $\mathfrak{G}_q$ and $\mathfrak{G}_q^+$ for every odd prime $q \leq 10^6$, thus enlarging the size of the previously known range for $\mathfrak{G}_q$ and $\mathfrak{G}_q^+$. Our method also reveals that difference $\mathfrak{G}_q - \mathfrak{G}_q^+$ can be computed in a much simpler way than both its summands. Moreover, as a by-product, we also computed $M_q = \max_{\chi\neq\chi_0} |L'/L(1,\chi)|$ for every odd prime $q \leq 10^6$, where $L(s,\chi)$ are the Dirichlet L-functions, χ run over the non trivial Dirichlet characters mod q and χ_0 is the trivial Dirichlet character mod q. As another by-product of our computations, we will also provide more data on the generalised Euler constants in arithmetic progressions.

[12] A. Languasco. Numerical verification of Littlewood's bounds for $|L(1,\chi)|$. *Journal of Number Theory*, 223:12–34, 2021. https://doi.org/10.1016/j.jnt.2020.12.017, MR:4213696, ZBL:07329220.

Abstract: Let $L(s,\chi)$ be the Dirichlet L-function associated to a non trivial primitive Dirichlet character χ defined mod q, where q is an odd prime. In this paper we introduce a fast method to compute $|L(1,\chi)|$ using the

values of Euler's Γ function. We also introduce an alternative way of computing $\log\Gamma(x)$ and $\psi(x) = \Gamma'/\Gamma(x)$, $x \in (0,1)$. Using such algorithms we numerically verify the classical Littlewood bounds and the recent Lamzouri-Li-Soundararajan estimates on $|L(1,\chi)|$, where χ runs over the non trivial primitive Dirichlet characters mod q, for every odd prime q up to 10^7. programs used and the results here described are collected at the following address http://www.math.unipd.it/~languasc/Littlewood_ineq.html.

[13] A. Languasco and L. Righi. A fast algorithm to compute the Ramanujan-Deninger Gamma function and some number-theoretic applications. *Math. Comp.*, 90:2899–2921, 2021. https://doi.org/10.1090/mcom/3668, MR:4305373; ZBL:07390221.

Abstract: We introduce a fast algorithm to compute the Ramanujan-Deninger gamma function and its logarithmic derivative at positive values. Such an algorithm allows us to greatly extend the numerical investigations about the Euler-Kronecker constants $\mathfrak{G}_q$, $\mathfrak{G}_q^+$ and $M_q = \max_{\chi\neq\chi_0}|L'/L(1,\chi)|$, where q is an odd prime, χ runs over the primitive Dirichlet characters mod q, χ_0 is the trivial Dirichlet character mod q and $L(s,\chi)$ is the Dirichlet L-function associated to χ. Using such algorithms we obtained that $\mathfrak{G}_{50040955631} = -0.16595399\ldots$ and $\mathfrak{G}^+_{50040955631} = 13.89764738\ldots$ thus getting a new negative value for $\mathfrak{G}_q$. Moreover we also computed $\mathfrak{G}_q$, $\mathfrak{G}_q^+$ and M_q for every odd prime q, $10^6 < q \le 10^7$, thus extending the results in proved by the first author in 2020. As a consequence we obtain that both $\mathfrak{G}_q$ and $\mathfrak{G}_q^+$ are positive for every odd prime q up to 10^7 and that $\frac{17}{20}\log\log q < M_q < \frac{5}{4}\log\log q$ for every odd prime $1531 < q \le 10^7$. In fact the lower bound holds true for $q > 13$. The programs used and the results here described are collected at the following address http://www.math.unipd.it/~languasc/Scomp-appl.html.

[14] A. Languasco and A. Zaccagnini. Sum of one prime power and two squares of primes in short intervals. *Rocky Mountain Journal of Mathematics*, 51:213–224, 2021. https://doi.org/10.1216/rmj.2021.51.213,MR:4280109, ZBL:07393760.

Abstract: Let $k \ge 1$ be an integer. We prove that a suitable asymptotic formula for the average number of representations of integers $n = p_1^k + p_2^2 + p_3^2$, where p_1, p_2, p_3 are prime numbers, holds in intervals shorter than the the ones previously known.

[15] M. Cantarini, A. Gambini, A. Languasco, and A. Zaccagnini. On a average ternary problem with prime powers. *The Ramanujan Journal*, 53:155–166, 2020. https://doi.org/10.1007/s11139-019-00237-x, MR:4148463, ZBL:07176138.

Abstract: We continue our work on averages for ternary additive problems with powers of prime numbers in short intervals by computing the average number of representations of a positive integer n as $p_1^{k_1} + p_2^{k_2} + p_3^{k_3}$, where p_1, p_2 and p_3 are prime numbers and $2 \le k_1 \le k_2 \le k_3$ are natural numbers.

[16] A. Languasco and A. Zaccagnini. Short intervals asymptotic formulae for binary problems with prime powers, II. *J. Aus. Math. Soc.*, 109:351–370, 2020. http://doi.org/10.1017/S1446788719000120, MR:4190085, ZBL:07286548.

Abstract: We improve the uniformity range of our results about the asymptotic formulae in short intervals for the average number of representations of integers of the forms $n = p_1^{\ell_1} + p_2^{\ell_2}$ and $n = p^{\ell_1} + m^{\ell_2}$, where $\ell_1, \ell_2 \ge 2$, p, p_1, p_2 are prime numbers and m is an integer.

[17] A. Languasco and A. Zaccagnini. A Cesàro average for an additive problem with prime powers. In *Proceedings of the conference "Number Theory Week", Poznań, September 4–8, 2017. Banach Center Publications, Institute of Matehematics, Polish Academy of Sciences, Warszawa*, volume 118, pages 137–152, 2019. http://dx.doi.org/10.4064/bc118-9, MR:3931260, ZBL:07087893.

Abstract: Let $1 \le \ell_1 \le \ell_2$ be two integers, Λ be the von Mangoldt function and $r_{\ell_1,\ell_2}(n) = \sum_{m_1^{\ell_1}+m_2^{\ell_2}=n}\Lambda(m_1)\Lambda(m_2)$ be the weighted counting function for the number of representation of an integer as a sum of two prime powers. We prove a suitable explicit formula, in terms of the non-trivial zeros of the Riemann zeta-function $\zeta(s)$, for the Cesàro average of weight $k > 1$ of $r_{\ell_1,\ell_2}(n)$.

[18] A. Languasco and A. Zaccagnini. A Cesàro average for generalised Hardy-Littlewood numbers. *Kodai Mathematical Journal*, 42:358–375, 2019. https://doi.org/10.2996/kmj/1562032834, MR:3981309, ZBL:07108016.

Abstract: Let $\ell \ge 1$ be an integer and where Λ is the von Mangoldt function. We prove a suitable explicit formula, in terms of the non-trivial zeros of the Riemann zeta-function $\zeta(s)$, for the Cesàro average of weight $k > 1$ of $r_{\ell,2}(n)$.

[19] A. Languasco and A. Zaccagnini. Sums of four prime cubes in short intervals. *Acta Math. Hungar.*, 159:150–163, 2019. http://doi.org/10.1007/s10474-019-00973-y, MR:4003700, ZBL:07119764.

Abstract: We prove that a suitable asymptotic formula for the average number of representations of integers $n = p_1^3 + p_2^3 + p_3^3 + p_4^3$, where p_1, p_2, p_3, p_4 are prime numbers, holds in intervals shorter than the the ones previously known.

[20] A. Gambini, A. Languasco, and A. Zaccagnini. A diophantine approximation problem with two primes and one k-power of a prime. *Journal of Number Theory*, 188:210–228, 2018. https://doi.org/10.1016/j.jnt.2018.01.002, MR:3778631, ZBL:06855844.

Abstract: We refine a result of the last two Authors on a Diophantine approximation problem with two primes and a k-th power of a prime which was only proved to hold for $1 < k < 4/3$. We improve the k-range to $1 < k \le 3$ by combining Harman's technique on the minor arc with a suitable estimate for the L^4-norm of the relevant exponential sum over primes.

[21] A. Languasco and A. Zaccagnini. Short intervals asymptotic formulae for binary problems with prime powers. *Journal de Théorie des Nombres de Bordeaux*, 30:609–635, 2018. https://doi.org/10.5802/jtnb.1041, MR:3891329, ZBL:3A07081564.

Abstract: We prove results about the asymptotic formulae in short intervals for the average number of representations of integers of the forms $n = p_1^{\ell_1} + p_2^{\ell_2}$ and $n = p^{\ell_1} + m^{\ell_2}$, where ℓ_1, ℓ_2 are fixed integers, p, p_1, p_2 are prime numbers and m is an integer.

[22] A. Languasco, A. Perelli, and A. Zaccagnini. An extended pair-correlation conjecture and primes in short intervals. *Trans. A.M.S.*, 369(6):4235–4250, 2017. https://doi.org/10.1090/tran/6835, MR:3624407, ZBL:06698813.

Abstract: In this paper we extend the well-known investigations of Montgomery and Goldston & Montgomery, concerning the pair-correlation function and its relations with the distribution of primes in short intervals, to a more general version of the pair-correlation function.

[23] A. Languasco and A. Zaccagnini. Cesàro average in short intervals for Goldbach numbers. *Proc. A.M.S.*, 145(10):4175–4186, 2017. https://doi.org/10.1090/proc/13645, MR:3690604, ZBL:06767077.

Abstract: Let Λ be the von Mangoldt function and $R(n) = \sum_{h+k=n} \Lambda(h)\Lambda(k)$. Let further N, H be two integers, $N \ge 2$, $1 \le H \le N$, and assume that the Riemann Hypothesis holds. Then

$$\sum_{n=N-H}^{N+H} R(n)\Big(1 - \frac{|n-N|}{H}\Big) = HN - \frac{2}{H}\sum_{\rho}\frac{(N+H)^{\rho+2} - 2N^{\rho+2} + (N-H)^{\rho+2}}{\rho(\rho+1)(\rho+2)}$$

$$+\mathcal{O}\Big(N\Big(\log\frac{2N}{H}\Big)^2 + H(\log N)^2\log(2H)\Big),$$

where $\rho = 1/2 + i\gamma$ runs over the non-trivial zeros of the Riemann zeta function $\zeta(s)$.

[24] A. Languasco and A. Zaccagnini. Il fascino discreto della teoria dei numeri. *Sapere*, 1:22–26, 2017. http://www.saperescienza.it/, http://dx.doi.org/10.12919/sapere.2017.01.3.

Abstract: Questo articolo è dedicato ad una delle branche più antiche della matematica, la teoria dei numeri, che si occupa delle proprietà dei numeri interi. Dalle equazioni diofantee ai numeri primi, questi argomenti apparentemente solo teorici hanno trovato numerose applicazioni.

[25] A. Languasco and A. Zaccagnini. Short intervals asymptotic formulae for binary problems with primes and powers, I: density 3/2. *The Ramanujan Journal*, 42:371–383, 2017. http://dx.doi.org/10.1007/s11139-016-9805-1, MR:3596938, ZBL:06692048.

Abstract: We prove that suitable asymptotic formulae in short intervals hold for the problems of representing an integer as a sum of a prime and a square, or a prime square. Such results are obtained both assuming the Riemann Hypothesis and in the unconditional case.

[26] A. Languasco. Applications of some exponential sums on prime powers: a survey. In *Proceedings of the "Terzo Incontro Italiano di Teoria dei Numeri", Scuola Normale Superiore, Pisa, 21-24 Settembre 2015. Rivista di Matematica della Università di Parma*, volume 7, pages 19–37, 2016. MR:3675401, ZBL:06760984.

Abstract: Let Λ be the von Mangoldt function and $N > 0$, $\ell \ge 1$ be two integers. We will see some results by the author and Alessandro Zaccagnini obtained using the original Hardy & Littlewood circle method function, *i.e.*

$$\widetilde{S}_\ell(\alpha) = \sum_{n=1}^{\infty}\Lambda(n)e^{-n^\ell/N}e(n^\ell\alpha),$$

where $e(x) = \exp(2\pi i x)$, instead of $S_\ell(\alpha) = \sum_{n=1}^{N} \Lambda(n) e(n^\ell \alpha)$. We will also motivate why, for some short interval additive problems, the approach using $\widetilde{S}_\ell(\alpha)$ gives sharper results than the ones that can be obtained with $S_\ell(\alpha)$.

[27] A. Languasco, A. Perelli, and A. Zaccagnini. An extension of the pair-correlation conjecture and applications. *Mathematical Research Letters*, 23(1):201–220, 2016. http://dx.doi.org/10.4310/MRL.2016.v23.n1.a10, MR:3512883, ZBL:06609432.

Abstract: We study an extension of Montgomery's pair-correlation conjecture and its relevance in some problems on the distribution of prime numbers.

[28] A. Languasco and A. Zaccagnini. A Diophantine problem with prime variables. In V. Kumar Murty, D. S. Ramana, and R. Thangadurai, editors, *Highly Composite: Papers in Number Theory, Proceedings of the International Meeting on Number Theory, celebrating the 60th Birthday of Professor R. Balasubramanian (Allahabad, 2011)*, volume 23 of *Ramanujan Math. Soc. Lect. Notes Ser.*, pages 157–168. Ramanujan Math. Soc., Mysore, 2016. MR:3692733.

[29] A. Languasco and A. Zaccagnini. Short intervals asymptotic formulae for binary problems with primes and powers, II: density 1. *Monatsh. Math.*, 181:419–435, 2016. http://dx.doi.org/10.1007/s00605-015-0871-z, MR:3539942, ZBL:1350.11089.

Abstract: We prove that suitable asymptotic formulae in short intervals hold for the problems of representing an integer as a sum of a prime square and a square, or a prime square. Such results are obtained both assuming the Riemann Hypothesis and in the unconditional case.

[30] A. Languasco and A. Zaccagnini. Sum of one prime and two squares of primes in short intervals. *Journal of Number Theory*, 159:45–58, 2016. http://dx.doi.org/10.1016/j.jnt.2015.07.010, MR:3412711, ZBL:06497366.

Abstract: Assuming the Riemann Hypothesis we prove that the interval $[N, N+H]$ contains an integer which is a sum of a prime and two squares of primes provided that $H \geq C(\log N)^4$, where $C > 0$ is an effective constant.

[31] A. Languasco and A. Zaccagnini. A Cesàro Average of Goldbach numbers. *Forum Mathematicum*, 27:1945–1960, 2015. http://dx.doi.org/10.1515/forum-2012-0100, MR:3365783, ZBL:06458901.

Abstract: Let Λ be the von Mangoldt function and $r_G(n) = \sum_{m_1+m_2=n} \Lambda(m_1)\Lambda(m_2)$ be the counting function for the Goldbach numbers. Let $N \geq 2$ be an integer. We prove that

$$\sum_{n\leq N} r_G(n) \frac{(1-n/N)^k}{\Gamma(k+1)} = \frac{N^2}{\Gamma(k+3)} - 2\sum_{\rho} \frac{\Gamma(\rho)}{\Gamma(\rho+k+2)} N^{\rho+1} + \sum_{\rho_1}\sum_{\rho_2} \frac{\Gamma(\rho_1)\Gamma(\rho_2)}{\Gamma(\rho_1+\rho_2+k+1)} N^{\rho_1+\rho_2} + \mathcal{O}_k(N),$$

for $k > 1$, where ρ, with or without subscripts, runs over the non-trivial zeros of the Riemann zeta-function $\zeta(s)$.

[32] A. Languasco and A. Zaccagnini. Explicit relations between primes in short intervals and exponential sums over primes. *Functiones et Approximatio, Commentarii Mathematici*, 51:379–391, 2014. http://dx.doi.org/10.7169/facm/2014.51.2.9, MR:3282634, ZBL:06380131.

Abstract: Under the assumption of the Riemann Hypothesis, we prove explicit quantitative relations between hypothetical error terms in the asymptotic formulae for truncated mean-square average of exponential sums over primes and in the mean-square of primes in short intervals. We also remark that such relations are connected with a more precise form of Montgomery's pair-correlation conjecture.

[33] A. Languasco and A. Zaccagnini. On a ternary diophantine problem with mixed powers of primes. *Acta Arithmetica*, 159:345–362, 2013. http://dx.doi.org/10.4064/aa159-4-4, MR:3080797, ZBL:06184261.

Abstract: Let $1 < k < 33/29$. We prove that if λ_1, λ_2 and λ_3 are non-zero real numbers, not all of the same sign and that λ_1/λ_2 is irrational and ϖ is any real number then, for any $\varepsilon > 0$ the inequality $\left|\lambda_1 p_1 + \lambda_2 p_2^2 + \lambda_3 p_3^k + \varpi\right| \leq \left(\max_j p_j\right)^{-(33-29k)/(72k)+\varepsilon}$ has infinitely many solution in prime variables $p_1, \ldots, p_3$.

[34] A. Languasco and A. Zaccagnini. A Cesàro Average of Hardy-Littlewood numbers. *J. Math. Anal. Appl.*, 401:568–577, 2013. http://dx.doi.org/10.1016/j.jmaa.2012.12.046, MR:3018008, ZBL:06156267.

Abstract: Let Λ be the von Mangoldt function and $r_{HL}(n) = \sum_{m_1+m_2^2=n} \Lambda(m_1)$, be the counting function for the Hardy-Littlewood numbers. Let N be a sufficiently large integer. We prove that

$$\sum_{n\le N} r_{HL}(n)\frac{(1-n/N)^k}{\Gamma(k+1)} = \frac{\pi^{1/2}}{2}\frac{N^{3/2}}{\Gamma(k+5/2)} - \frac{1}{2}\frac{N}{\Gamma(k+2)} - \frac{\pi^{1/2}}{2}\sum_{\rho}\frac{\Gamma(\rho)}{\Gamma(k+3/2+\rho)}N^{1/2+\rho} + \frac{1}{2}\sum_{\rho}\frac{\Gamma(\rho)}{\Gamma(k+1+\rho)}N^{\rho} + \frac{N^{3/4-k/2}}{\pi^{k+1}}\sum_{\ell\ge1}\frac{J_{k+3/2}(2\pi\ell N^{1/2})}{\ell^{k+3/2}} - \frac{N^{1/4-k/2}}{\pi^k}\sum_{\rho}\Gamma(\rho)\frac{N^{\rho/2}}{\pi^{\rho}}\sum_{\ell\ge1}\frac{J_{k+1/2+\rho}(2\pi\ell N^{1/2})}{\ell^{k+1/2+\rho}} + \mathcal{O}_k\left(N^{1/2}\right),$$

for $k > 1$, where ρ runs over the non-trivial zeros of the Riemann zeta-function $\zeta(s)$ and $J_\nu(u)$ denotes the Bessel function of complex order ν and real argument u.

[35] A. Languasco, A. Perelli, and A. Zaccagnini. Explicit relations between pair correlation of zeros and primes in short intervals. *J. Math. Anal. Appl.*, 394:761–771, 2012. http://dx.doi.org/10.1016/j.jmaa.2012.04.058, MR:2927496, ZBL:06062862.

Abstract: In this paper we obtain a quantitative version of the celebrated theorem by D.A. Goldston and H.L. Montgomery about the equivalence between the asymptotic behaviors of the mean-square of primes in short intervals and of the pair-correlation function of the zeros of the Riemann zeta function.

[36] A. Languasco and V. Settimi. On a Diophantine problem with one prime, two squares of primes and s powers of two. *Acta Arithmetica*, 154:385–412, 2012. http://dx.doi.org/10.4064/aa154-4-4, MR:2949876, ZBL:06055436.

Abstract: We refine a result of W.P. Li and Wang on the values of the form $\lambda_1 p_1+\lambda_2 p_2^2+\lambda_3 p_3^2+\mu_1 2^{m_1}+\cdots+\mu_s 2^{m_s}$, where p_1, p_2, p_3 are prime numbers, $m_1, \dots, m_s$ are positive integers, $\lambda_1, \lambda_2, \lambda_3$ are nonzero real numbers, not all of the same sign, λ_2/λ_3 is irrational and $\lambda_i/\mu_i \in \mathbb{Q}$, for $i \in \{1, 2, 3\}$.

[37] A. Languasco and A. Zaccagnini. A Diophantine problem with a prime and three squares of primes. *Journal of Number Theory*, 132:3016–3028, 2012. http://dx.doi.org/10.1016/j.jnt.2012.06.015, MR:2965205, ZBL:06097276.

Abstract: We refine a recent result of Li-Wang on the values of the form $\lambda_1 p_1 + \lambda_2 p_2^2 + \lambda_3 p_3^2 + \lambda_4 p_4^2$, where p_1, p_2, p_3, p_4 are prime numbers, $\lambda_1, \lambda_2, \lambda_3, \lambda_4$ are nonzero real numbers, not all of the same sign, and λ_1/λ_2 is irrational.

[38] A. Languasco and A. Zaccagnini. Sums of many primes. *J. Number Theory*, 132:1265–1283, 2012. http://dx.doi.org/10.1016/j.jnt.2011.11.004, MR:2899803, ZBL:06031097.

Abstract: Assuming that the Generalized Riemann Hypothesis (GRH) holds, we prove an explicit formula for the number of representations of an integer as a sum of $k \ge 5$ primes. Our error terms in such a formula improve by some logarithmic factors an analogous result by Friedlander-Goldston.

[39] A. Languasco and A. Zaccagnini. The number of Goldbach representations of an integer. *Proc. Amer. Math. Soc.*, 140:795–804, 2012. http://dx.doi.org/10.1090/S0002-9939-2011-10957-2, MR:2869064, ZBL:1252.11078.

Abstract: Let Λ be the von Mangoldt function and $R(n) = \sum_{h+k=n} \Lambda(h)\Lambda(k)$ be the counting function for the Goldbach numbers. Let $N \ge 2$ and assume that the Riemann Hypothesis holds. We prove that

$$\sum_{n=1}^{N} R(n) = \frac{N^2}{2} - 2\sum_{\rho}\frac{N^{\rho+1}}{\rho(\rho+1)} + \mathcal{O}\left(N\log^3 N\right),$$

where $\rho = 1/2 + i\gamma$ runs over the non-trivial zeros of the Riemann Zeta-function $\zeta(s)$. This improves a recent result by Bhowmik and Schlage-Puchta.

[40] D. Bazzanella, A. Languasco, and A. Zaccagnini. Prime numbers in logarithmic intervals. *Trans. Amer. Math. Soc.*, 362:2667–2684, 2010. http://dx.doi.org/10.1090/S0002-9947-09-05009-0, MR:2584615, ZBL:1200.11072.

Abstract: Let X be a large parameter. We will first give a new estimate for the integral moments of primes in short intervals of the type $(p, p + h]$, where $p \le X$ is a prime number and $h = o(X)$. Then we will apply this to prove that for every $\lambda > 1/2$ there exists a positive proportion of primes $p \le X$ such that the interval $(p, p + \lambda \log X]$ contains at least a prime number. As a consequence we improve Cheer and Goldston's result on the size of real numbers $\lambda > 1$ with the property that there is a positive proportion of integers $m \le X$ such that the interval $(m, m + \lambda \log X]$ contains no primes. We also prove other results concerning the moments of

the gaps between consecutive primes and about the positive proportion of integers $m \le X$ such that the interval $(m, m + \lambda \log X]$ contains at least a prime number. The last application of these techniques are two theorems (the first one unconditional and the second one in which we assume the validity of the Riemann Hypothesis and of a form of the Montgomery pair correlation conjecture) on the positive proportion of primes $p \le X$ such that the interval $(p, p + \lambda \log X]$ contains no primes.

[41] A. Languasco, A. Perelli, and A. Zaccagnini. On the Montgomery-Hooley theorem in short intervals. *Mathematika*, 52:231–243, 2010. http://dx.doi.org/10.1112/S0025579310000628, MR:2678027, ZBL:1238.11087.

Abstract: We study a short-interval version of a result due to Montgomery and Hooley. Write

$$S(x,h,Q) = \sum_{q\le Q} \sum_{\substack{a=1\\(a,q)=1}}^{q} \left|\psi(x+h;q,a) - \psi(x;q,a) - \frac{h}{\varphi(q)}\right|^2$$

and $\kappa = 1 + \gamma + \log 2\pi + \sum_p (\log p)/p(p-1)$. Denote the expected main term by $M(x,h,Q) = hQ\log(xQ/h) + (x+h)Q\log(1+h/x) - \kappa hQ$. Let ϵ, $A > 0$ be arbitrary, $x^{7/12+\epsilon} \le h \le x$ and $Q \le h$. There exists a positive constant c_1 such that

$$S(x,h,Q) - M(X,h,Q) \ll h^{1/2}Q^{3/2}\exp\left(-c_1\frac{(\log 2h/Q)^{3/5}}{(\log\log 3h/Q)^{1/5}}\right) + h^2\log^{-A}x.$$

Now assume *GRH* and let $\epsilon > 0$, $x^{1/2+\epsilon} \le h \le x$ and $Q \le h$. There exists a positive constant c_2 such that

$$S(x,h,Q) - M(x,h,Q) \ll \left(\frac{h}{Q}\right)^{1/4+\epsilon} Q^2 + hx^{1/2}\log^{c_2}x.$$

[42] A. Languasco and A. Zaccagnini. Computing the Mertens and Meissel-Mertens constants for sums over arithmetic progressions. *Experimental Mathematics*, 19:279–284, 2010. With an appendix by Karl K. Norton. http://dx.doi.org/10.1080/10586458.2010.10390624, MR:2743571, ZBL:06074851.

Abstract: We give explicit numerical values with 100 decimal digits for the Mertens constant involved in the asymptotic formula for $\sum_{\substack{p\le x\\ p\equiv a \bmod q}} 1/p$ and, as a by-product, for the Meissel-Mertens constant defined as $\sum_{p\equiv a \bmod q}(\log(1-1/p) + 1/p)$, for $q \in \{3, \dots, 100\}$ and $(q,a) = 1$.The complete set of results can be downloaded from the webpage: http://www.math.unipd.it/~languasc/Mertens-comput.html

[43] A. Languasco and A. Zaccagnini. On a Diophantine problem with two primes and s powers of two. *Acta Arith.*, 145:193–208, 2010. http://dx.doi.org/10.4064/aa145-2-7, MR:2733083, ZBL:1222.11049.

Abstract: We refine a recent result of Parsell on the values of the form $\lambda_1 p_1 + \lambda_2 p_2 + \mu_1 2^{m_1} + \cdots + \mu_s 2^{m_s}$, where p_1, p_2 are prime numbers, $m_1, \dots, m_s$ are positive integers, λ_1/λ_2 is negative and irrational and λ_1/μ_1, $\lambda_2/\mu_2 \in \mathbb{Q}$.

[44] A. Languasco and A. Zaccagnini. On the constant in the Mertens product for arithmetic progressions. I. Identities. *Functiones et Approximatio, Commentarii Mathematici*, 42:17–27, 2010. http://dx.doi.org/10.7169/facm/1269437065, MR:2640766, ZBL:1206.11112.

Abstract: We give new identities for the constants in the Mertens product over primes in the arithmetic progressions a mod q, extending previous work by Uchiyama, Grosswald, Williams and Moree.

[45] A. Languasco. A conditional result on the exceptional set for Hardy-Littlewood numbers in short intervals. *International Journal of Number Theory*, 5:933–951, 2009. http://dx.doi.org/10.1142/S179304210900247X, MR:2569737, ZBL:1251.11068.

Abstract: Assuming the Generalized Riemann Hypothesis holds, we prove some conditional estimates on the exceptional set in short intervals for the Hardy-Littlewood problem.

[46] A. Languasco and A. Zaccagnini. On the constant in the Mertens product for arithmetic progressions. II. Numerical values. *Math. Comp.*, 78:315–326, 2009. http://dx.doi.org/10.1090/S0025-5718-08-02148-0, MR:2448709, ZBL:1214.11108.

Abstract: We give explicit numerical values with 100 decimal digits for the constant in the Mertens product over primes in the arithmetic progressions a mod q, for $q \in \{3, \dots, 100\}$ and $(a,q) = 1$.

[47] A. Languasco and A. Zaccagnini. On the Hardy-Littlewood problem in short intervals. *Int. J. Number Theory*, 4:715–723, 2008. http://dx.doi.org/10.1142/S179304210800164X, MR:2458837, ZBL:1251.11069.

Abstract: In this paper we will study the distribution of Hardy-Littlewood numbers in short intervals both unconditionally and conditionally, *i.e.* assuming the Riemann Hypothesis (RH). Our results concern the average of the asymptotic formula for the number of representations of an HL-number in almost all short intervals.

[48] A. Languasco and A. Zaccagnini. Some estimates for the average of the error term of the Mertens product for arithmetic progressions. *Funct. Approx. Comment. Math.*, 38:41–47, 2008. http://dx.doi.org/10.7169/facm/1229624650, MR:2433787, ZBL:1233.11100.

Abstract: We give estimates for the error term of the Mertens product over primes in arithmetic progressions of the Bombieri–Vinogradov and Barban–Davenport–Halberstam type.

[49] A. Languasco, J. Pintz, and A. Zaccagnini. On the sum of two primes and k powers of two. *Bull. London Math. Soc.*, 39:771–780, 2007. http://dx.doi.org/10.1112/blms/bdm062, MR:2365226, ZBL:1137.11066.

Abstract: Let X be a large integer. We prove that, for any fixed positive integer k, a suitable asymptotic formula for the number of representations of an even integer $N \in [1, X]$ as the sum of two primes and k powers of 2 holds with at most $\mathcal{O}_k\left(X^{3/5}(\log X)^{10}\right)$ exceptions.

[50] A. Languasco and A. Zaccagnini. A note on Mertens' formula for arithmetic progressions. *Journal of Number Theory*, 127:37–46, 2007. http://dx.doi.org/10.1016/j.jnt.2006.12.015, MR:2351662, ZBL:1210.11105.

Abstract: We study the Mertens product over primes in arithmetic progressions, and find a uniform version of previous results on the asymptotic formula, improving at the same time the size of the error term, and giving an alternative, simpler value for the constant appearing in the main term.

[51] A. Languasco. On the sum of a prime and a k-free number. *Functiones et Approximatio, Commentarii Mathematici*, 34:19–26, 2005. http://www.staff.amu.edu.pl/~fa/XXXIV/fa-34-1-019.pdf, MR:2269661, ZBL:1228.11156.

Abstract: We prove an asymptotic formula (that refines old results by Walfisz and Mirsky) for the number of representations of sufficiently large integer as a sum of a prime and a k-free number, $k \geq 2$.

[52] A. Languasco. Primos Gemelos. *La Voz de Almeria, Seccion Matematica*, 2005. (pubblicato il 04/09/2005 in lingua spagnola, traduzione di Juan Cuadra Diaz).

Abstract: Breve articolo divulgativo riguardante la congettura dei primi gemelli.

[53] A. Languasco. On the exceptional set for Hardy-Littlewood's numbers in short intervals. *Tsukuba J. Math.*, 28:169–192, 2004. https://tsukuba.repo.nii.ac.jp/?action=repository_uri&item_id=18386&file_id=17&file_no=1, MR:2082228, ZBL:1068.11066. *Corrigendum ibid.*, https://tsukuba.repo.nii.ac.jp/?action=repository_uri&item_id=29695&file_id=17&file_no=1, Tsukuba Journal of Mathematics, **30** (2006), 237–240, MR:2248294, ZBL:1201.11095.

Abstract: In 1923 Hardy and Littlewood conjectured that every sufficiently large integer is either a k-power of an integer or a sum of a prime and a k-power of an integer, for $k = 2, 3$. We will call HL-numbers the integers that are a sum of a prime and a k-power of an integer. Let now $k \geq 2$ and denote by E_k the set of integers which are neither an HL-number nor a power of an integer. Here we prove that there exists an absolute positive constant δ such that for $H \geq X^{7/12(1-\frac{1}{k})+\delta}$

$$|E_k(X, H)| \ll H^{1-\delta/(5K)},$$

where $K = 2^{k-2}$, thus improving previous results by Perelli-Pintz, Mikawa, Perelli-Zaccagnini and Zaccagnini. In the Corrigendum we correct a mistake the treatment of the case $k = 2$.

[54] A. Languasco. On the exceptional set of Goldbach's problem in short intervals. *Monatsh. Math.*, 141:147–169, 2004. http://dx.doi.org/10.1007/s00605-003-0038-1, MR:2037990, ZBL:1059.11059.

Abstract: Let E be the set of integers which are not a sum of two primes, $E(X) = E \cap [1, X]$ and $E(X, H) = E \cap [X, X + H]$, where $H = o(X)$. A well known result of Montgomery-Vaughan proves that there exists an absolute positive constant δ such that $|E(X)| \ll X^{1-\delta}$. Here we prove that there exists an absolute positive constant δ such that, for $H \geq X^{7/24+7\delta}$, $|E(X, H)| \ll H^{1-\delta/600}$, improving a result by Peneva.

[55] A. Languasco. The exceptional set in short intervals for two additive problems with primes: a survey. *Riv. Mat. Univ. Parma (7)*, 3*:223–231, 2004. MR:2128851, ZBL:1166.11348.

Abstract: We give a brief account about the exceptional sets in short intervals for the Goldbach and the Hardy-Littlewood problems. In particular, we present two recent results about Montgomery-Vaughan's type estimates for such exceptional sets.

[56] A. Languasco, F. Menegazzo, and M. Morigi. On the composition length of finite primitive linear groups. *Arch. Math.*, 79:408–417, 2002. http://dx.doi.org/10.1007/BF02638376, MR:1966776, ZBL:1015.20034.

Abstract: Let G be a finite primitive linear group over a field K, where K is a finite field or a field of numbers. We bound the composition length of G in terms of the dimension of the underlying vector space and of the degree of K over its prime subfield. As a by-product, we prove a result of number theory which bounds thenumber of prime factors (counting moltiplicities), of $q^n - 1$, where $q, n > 1$ are integers, improving a result of Turull and Zame.

[57] A. Languasco and A. Perelli. Crittografia e firma digitale. In M. Emmer and M. Manaresi, editors, *Matematica, Arte, Tecnologia, Cinema*, pages 99–106, Bologna, 2002. Springer-Verlag, Milano. trad. inglese in *Mathematics, Art, Technology, and Cinema*, Springer-Verlag, Berlin, Heidelberg, New York, 2003.

Abstract: La sicurezza nella trasmissione dell'informazione è una necessità da sempre sentita dall'umanità. Nel corso dei secoli sono state utilizzate varie idee per questo scopo; esempi famosi sono il metodo di trasposizione di Giulio Cesare e la macchina di cifratura Enigma (utilizzata dalle forze armate tedesche durante la seconda guerra mondiale). I tentativi fatti precedentemente agli anni '70 non furono completamente soddisfacenti (si ricordi ad esempio la storia della forzatura del codice Enigma operata dal matematico A. Turing e dal suo gruppo negli anni '40); la possibilità di costruire un sistema crittografico rispondente a requisiti di sicurezza e autenticità fu provata a livello teorico da Diffie e Hellman nel 1976, mediante un rivoluzionario metodo detto a chiave pubblica. Tale idea trovò applicazione pratica due anni dopo, quando Rivest, Shamir e Adleman, utilizzando le proprietà dei numeri primi, concretizzarono l'idea di Diffie e Hellman. La crittografia moderna nasce quindi negli anni '70, e soppianta quasi completamente i metodi ottenuti come evoluzione delle idee classiche perché consente varie altre applicazioni. Ad esempio, la crittografia a chiave pubblica permette la costruzione di algoritmi efficienti e sicuri per l'autenticazione di documenti elettronici, ossia apre il campo ad una definizione di firma digitale.

[58] D. Bazzanella and A. Languasco. On the asymptotic formula for Goldbach numbers in short intervals. *Studia Sci. Math. Hungar.*, 36:185–199, 2000. http://dx.doi.org/10.1556/SScMath.36.2000.1-2.14, MR:1768230, ZBL:0973.11089.

Abstract: Let $R(k) = \sum_{l+m=k} \Lambda(l)\Lambda(m)$, $\mathfrak{S}(k) = 2 \prod_{p>2} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{\substack{p|k \\ p>2}} \left(\frac{p-1}{p-2}\right)$ if k is even and $\mathfrak{S}(k) = 0$ if k is odd. It is known that $R(k) \sim k\mathfrak{S}(k)$ as $N \to \infty$ for almost all $k \in [N, 2N]$ and that

$$\sum_{k\in[n,n+H)} R(k) \sim \sum_{k\in[n,n+H)} k\mathfrak{S}(k) \quad \text{for} \quad n \to \infty \tag{1}$$

uniformly for $H \geq n^{1/6+\epsilon}$. Here we prove, assuming $N^\epsilon \leq H \leq N^{1/6+\epsilon}$ and $N \to \infty$, that (1) holds for almost all $n \in [N, 2N]$.

[59] J. Kaczorowski, A. Languasco, and A. Perelli. A note on Landau's formula. *Funct. Approx. Comment. Math.*, 28:173–186, 2000. Dedicated to Włodzimierz Staś on the occasion of his 75th birthday. http://www.staff.amu.edu.pl/~fa/XXVIII/fa-28-1-173.pdf, MR:1824002, ZBL:1034.11049.

Abstract: Landau proved, for any fixed $x > 1$, that

$$\sum_{0<\gamma\leq T} x^\rho = -\frac{T}{2\pi}\Lambda(x) + O(\log T) \quad \text{for} \quad T \to \infty,$$

where ρ runs over the non-trivial zeros of the Riemann zeta function $\zeta(s)$ and $\Lambda(x) = \log p$ if $x = p^m$, p prime and $\Lambda(x) = 0$ otherwise. Recently Gonek has obtained a form of the previous formula which is uniform in T and x. Here we furnish a uniform version of Landau's formula in which the error term has sharper individual and mean-square estimates.

[60] A. Languasco. An Introduction to Cryptography. *Queen's Papers in Pure and Applied Mathematics*, 119(121-140), 2000. in The Curves Seminar at Queen's , vol. 13, ed. da A.V. Geramita.

Abstract: In this introduction to Cryptography, we start by giving some basic notions from elementary number theory and see how they can be applied to send secret messages. After introducing congruence theory, Fermat's little theorem and the Euler-Fermat theorem, we examine, from a historical point of view, some classic cryptographic systems. Then we give the main properties of modern cryptographic systems and, in particular, we define public key cryptography. One of the most important public-key systems (which exploits the fact that in $\mathbb{Z}$ primality algorithms are much faster than factorization ones) is presented: the R.S.A. cryptosystem. We also present another public key system which exploits the discrete logarithm problem and which is also consistently used as

an alternative to R.S.A. (for example the U.S. government offices use it for their digital signature scheme). An analogue of the discrete logarithm problem is used in the so-called elliptic curves cryptosystems . Unfortunately, the amount of mathematical theory needed to understand the elliptic curves method is too great to be explained here. So, we will say, in the last paragraph, just a few words on the differences between the discrete logarithm problem and its elliptic curve analogue. This article is geared toward the amateur interested in the subject.

[61] A. Languasco. Some refinements of error terms estimates for certain additive problems with primes. *J. Number Theory*, 81:149–161, 2000. http://dx.doi.org/10.1006/jnth.1999.2468, MR:1743499, ZBL:1003.11047.

Abstract: We study, under the assumption of the Generalized Riemann Hypothesis, the individual and mean-square error terms for the number of integers representable as a sum of $k \geq 3$ primes. We improve, using a smoothing technique, Friedlander-Goldston's recent results on this topic. Moreover, we remark that the argument we use can also be applied to other similar problems.

[62] A. Languasco and A. Perelli. Pair correlation of zeros, primes in short intervals and exponential sums over primes. *J. Number Theory*, 84:292–304, 2000. http://dx.doi.org/10.1006/jnth.2000.2511, MR:1796516, ZBL:0973.11081.

Abstract: Assume the Riemann Hypothesis and let $F(X,T) = 4 \sum_{0<\gamma_1,\gamma_2\leq T} \frac{X^{i(\gamma_1-\gamma_2)}}{4+(\gamma_1-\gamma_2)^2}$, where γ_j, $j = 1, 2$, run over the imaginary part of the non-trivial zeros of the Riemann zeta-function, be the Montgomery's pair correlation function. Goldston-Montgomery proved, for any $\epsilon > 0$, that $F(X,T) \sim \frac{1}{2\pi} T \log T$ uniformly for $X^{\epsilon} \leq T \leq X$ is equivalent to $J(X,H) \sim HX \log \frac{X}{H}$ uniformly for $1 \leq H \leq X^{1-\epsilon}$ where $J(X,H)$ is Selberg's integral. Here we prove, for any $\epsilon > 0$, that $F(X,T) \sim \frac{1}{2\pi} T \log T$ uniformly for $X^{1/2+\epsilon} \leq T \leq X$ is equivalent to a suitable asymptotic formula for the truncated mean-square of exponential sums over primes.

[63] A. Languasco and A. Perelli. Numeri Primi e Crittografia. In M. Emmer, editor, *Matematica e Cultura 2000*, pages 227–233, Venezia, 2000. Springer-Verlag, Milano. trad. inglese in *Mathematics and Culture I*, Springer-Verlag, Berlin, Heidelberg, New York, 2003.

Abstract: Da una parte lo studio dei numeri, in particolare dei numeri primi, ha affascinato i matematici fin dalle epoche più antiche; d'altra parte, la sicurezza nella comunicazione dell'informazione é una necessità da sempre sentita dall'umanità. Negli ultimi vent'anni, grazie alla scoperta di nuovi metodi matematici e al notevole progresso nel campo dei computers, si é gradualmente sviluppato uno stretto rapporto tra le due discipline. Attualmente i metodi più sicuri per la trasmissione dell'informazione, che hanno recentemente avuto nuovo impulso dallo sviluppo del commercio elettronico, si basano su algoritmi che dipendono da notevoli proprietà dei numeri primi. In questo intervento tratteggeremo dapprima alcuni elementi dello sviluppo della teoria dei numeri primi; descriveremo poi un'applicazione al problema della sicurezza nella trasmissione dell'informazione, ossia alla crittografia.

[64] A. Languasco. A conditional result on Goldbach numbers in short intervals. *Acta Arith.*, 83:93–103, 1998. https://eudml.org/doc/207117, MR:1490641, ZBL:0940.11045.

Abstract: Assume the Riemann Hypothesis and a weaker form of Montgomery's pair correlation conjecture, i.e., for every $\theta \in [1, 2)$

$$F(X,T) = 4 \sum_{0<\gamma_1,\gamma_2\leq T} \frac{X^{i(\gamma_1-\gamma_2)}}{4+(\gamma_1-\gamma_2)^2} \ll T(\log T)^{\theta},$$

where γ_j, $j = 1, 2$, run over the imaginary part of the non-trivial zeros of the Riemann zeta-function, holds uniformly for $\frac{X}{H} \leq T \leq X$, where $1 \leq H \leq X$. Then, for all sufficiently large X and $H \gg (\log X)^{\theta}$, we have that the interval $[X, X+H]$ contains a even integer which is a sum of two primes.

[65] A. Languasco. A note on primes and Goldbach numbers in short intervals. *Acta Math. Hungar.*, 79:191–206, 1998. http://dx.doi.org/10.1023/A:1006553707162, MR:1616038, ZBL:0940.11046.

Abstract: Let $J(N,H)$ be the Selberg integral and $E(x,T)$ the error term in Kaczorowski-Perelli's weighted form of the classical explicit formula. We prove that the estimate $J(N,H) = o(H^2N)$ is connected with an appropriate estimate of $\int_N^{2N} |E(x,T)|^2 dx$, uniformly for H and T in some ranges. Moreover, assuming a suitable bound for the quantity $\int_N^{2N} |E(x,T)|^2 dx$, we also obtain, for all sufficiently large N and $H \gg (\log N)^{11/2}$, that every interval $[N, N+H]$ contains $\gg H$ Goldbach numbers.

[66] A. Languasco. A singular series average and Goldbach numbers in short intervals. *Acta Arith.*, 83:171–179, 1998. https://eudml.org/doc/207113, MR:1490647, ZBL:0894.11037.

Abstract: Let $\mathfrak{S}(n) = 2\prod_{p>2}\left(1-\frac{1}{(p-1)^2}\right)\prod_{\substack{p|n\\p>2}}\left(\frac{p-1}{p-2}\right)$ if n is even and $\mathfrak{S}(n)=0$ if n is odd, be the singular series of the Goldbach problem. Let $\nu \geq 1$ be a fixed real number. We prove that

$$\sum_{n\leq X}\mathfrak{S}(n)^\nu = c_1 X + c_2(\log X)^\nu + O((\log X)^{\nu-1/3}),$$

where c_1, c_2 and the implicit constant depend on ν. As a consequence, we improve the known results on the positive proportion of Goldbach numbers in short intervals.

[67] A. Languasco and A. Perelli. A pair correlation hypothesis and the exceptional set in Goldbach's problem. *Mathematika*, 43:349–361, 1996. http://dx.doi.org/10.1112/S0025579300011827, MR:1433280, ZBL:0884.11042.

Abstract: Let

$$E(X,H) = |\{2n \in [X, X+H] : 2n \text{ is not a sum of two primes}\}|$$

be the exceptional set for Goldbach's problem in short intervals. We will assume the Generalized Riemann Hypothesis and that, for $(a,q)=1$, $\epsilon>0$ and $\theta \in (0,\frac{1}{2}]$ fixed,

$$F(X,T;q,a) = \sum_{\chi_1,\chi_2 \pmod q}\chi_1(a)\overline{\chi}_2(a)\tau(\overline{\chi}_1)\tau(\chi_2)\sum_{|\gamma_1|,|\gamma_2|\leq T}X^{i(\gamma_1-\gamma_2)}w(\gamma_1-\gamma_2) \ll q^2 T X^\epsilon,$$

where $w(u)=\frac{4}{4+u^2}$, $\tau(\chi)$ denotes the Gauss sum and γ_j, $j=1,2$, run over the imaginary part of the non trivial zeros of $L(s,\chi_j)$, holds uniformly for $\frac{X^{1-\theta}}{q}\leq T\leq X$ and $q\leq X^\theta$. Under the previous hypotheses we prove, for every $\epsilon>0$ fixed, that

$$E(X, X^{2\theta}) \ll_\epsilon X^\epsilon,$$

i.e. for $\theta > \frac{\epsilon}{2}$ all even integers in any interval of the form $[X, X+X^{2\theta}]$ but $O(X^\epsilon)$ exceptions are a sum of two primes.

[68] A. Languasco. Some results on Goldbach's problem. *Rend. Sem. Mat. Univ. Politec. Torino*, 53(4):325–337, 1995. http://seminariomatematico.dm.unito.it/rendiconti/cartaceo/53-4/325.pdf, MR:1452389, ZBL:0882.11055.

Abstract: In Section 1 we introduce the Goldbach Conjecture and give a brief account on the main contribution to this subject. In the other sections we sketch the proofs of some results on the existence of Goldbach numbers in short intervals and on the exceptional set for Goldbach's problem.

[69] A. Languasco and A. Perelli. On Linnik's theorem on Goldbach numbers in short intervals and related problems. *Ann. Inst. Fourier*, 44:307–322, 1994. http://dx.doi.org/10.5802/aif.1399, MR:1296733, ZBL:0799.11040.

Abstract: Linnik proved, assuming the Riemann Hypothesis, that for any $\varepsilon>0$, the interval $[N, N+\log^{3+\varepsilon}N]$ contains a number which is the sum of two primes, provided that N is sufficiently large. This has subsequently been improved to the same assertion being valid for the smaller gap $C\log^2 N$, the added new ingredient being Selberg's estimate for the mean-square of primes in short intevals. Here we give another proof of this sharper result which avoids the use of Selberg's estimate and is therefore more in the spirit of Linnik's original approach. We also improve an unconditional result of Lavrik's on truncated forms of Parseval's identity for exponential sums over primes.

WEB-PAPERS

[70] A. Languasco and A. Zaccagnini. Alcune proprietà dei numeri primi, I. *Sito web Bocconi-Pristem*, 2005. http://matematica-old.unibocconi.it/LangZac/home.htm.

Abstract: È il primo di una serie di articoli divulgativi in cui si raccolgono proprietà dei numeri primi che di solito non si trovano nei libri di testo. In particolare, si parla del Teorema Fondamentale dell'Aritmetica, del Crivello di Eratostene e della densità dei primi nella successione dei numeri naturali. In Appendice si danno risultati piú complessi.

[71] A. Languasco and A. Zaccagnini. Alcune proprietà dei numeri primi, II. *Sito web Bocconi-Pristem*, 2005. http://matematica-old.unibocconi.it/LangZac/home2.htm.

Abstract: È il secondo di una serie di articoli divulgativi in cui si raccolgono proprietà dei numeri primi che di solito non si trovano nei libri di testo. Qui parliamo di criteri di primalità ed algoritmi di fattorizzazione, di certificati di primalità, di numeri primi di forma speciale. Anche qui, risultati piú complessi sono dati in Appendice.

[72] A. Languasco and A. Zaccagnini. Esistono piccoli intervalli fra primi consecutivi! *Sito web Bocconi-Pristem*, 2005. http://matematica-old.unibocconi.it/LangZac/risultatoteorianumeri.htm.

Abstract: Questo articolo è un breve annuncio per pubblicizzare un importante recente risultato di Goldston, Pintz e Yıldırım sull'esistenza di piccoli intervalli tra numeri primi consecutivi, ossia sul fatto che $\liminf (p_{n+1} - p_n)/\log p_n = 0$, dove p_n indica l'n-esimo numero primo.

[73] A. Languasco and A. Zaccagnini. Intervalli fra numeri primi consecutivi. *Sito web Bocconi-Pristem*, 2005. http://matematica-old.unibocconi.it/LangZac/introduzione3.htm.

Abstract: Questo articolo descrive lo stato dell'arte riguardo la questione degli intervalli fra numeri primi consecutivi, nei due casi di grandi o piccole deviazioni dal comportamento medio. Dimostriamo alcuni risultati che, pur non essendo i migliori oggi noti, sono pur sempre non banali e illustrano bene le tecniche che si usano in questo campo. Questo articolo si rivolge a studenti universitari.

Other Publications

[74] A. Languasco. Codici a chiave pubblica ed Algoritmi di Primalità. Master's thesis, Università di Genova, 1989. (italian).

[75] A. Languasco. *La congettura di Goldbach*. PhD thesis, Politecnico di Torino, Università di Torino, Università di Genova, 1995. (italian).

[76] A. Languasco. Dispense di Analisi Matematica 1. Lecture Notes, Manuscript, (italian), 1999.

[77] A. Languasco. Dispense di Algebra Lineare, Geometria e Calcolo Differenziale in più variabili (Matematica B). Lecture Notes, Manuscript, (italian), 2002.

[78] B. Bruno and A. Languasco. Dispense integrative per il Corso di Istituzioni di Analisi Matematica II. Lecture Notes, Manuscript, (italian), 2003.

[79] A. Languasco. Dispense per il Corso di Metodi Matematici per la Statistica (parte di Analisi Matematica). Lecture Notes, Manuscript, (italian), 2005.

[80] A. Languasco. Dispense per il Corso di Fondamenti di Analisi Matematica 2. Lecture Notes, Manuscript, (italian), 2020.

Prof. Alessandro Languasco, Ph. D.
Indirizzo Dipartimento di Matematica "Tullio Levi-Civita", via Trieste 63, 35121 Padova
e-mail alessandro.languasco@unipd.it
pagina web http://www.math.unipd.it/~languasc

Padova, November 20, 2021

Alessandro LANGUASCO