TURUN
YLIOPISTO
UNIVERSITY
OF TURKU

PROBLEMS IN ANALYTIC AND ALGEBRAIC NUMBER THEORY

Olli Järviniemi

TURUN YLIOPISTON JULKAISUJA – ANNALES UNIVERSITATIS TURKUENSIS
SARJA – SER. AI OSA – TOM. 694 | ASTRONOMICA – CHEMICA – PHYSICA – MATHEMATICA | TURKU 2023

TURUN
YLIOPISTO
UNIVERSITY
OF TURKU

PROBLEMS IN ANALYTIC AND ALGEBRAIC NUMBER THEORY

Olli Järviniemi

TURUN YLIOPISTON JULKAISUJA – ANNALES UNIVERSITATIS TURKUENSIS
SARJA – SER. AI OSA – TOM. 694 | ASTRONOMICA - CHEMICA - PHYSICA – MATHEMATICA | TURKU 2023

University of Turku

Faculty of Science
Department of Mathematics and Statistics
Mathematics
Doctoral programme in Exact Sciences (EXACTUS)

Supervised by

Professor Kaisa Matomäki
University of Turku

Docent Joni Teräväinen
University of Turku

Reviewed by

Professor Stephan Baier
RKM Vivekananda University
India

Doctor Pieter Moree
Max Planck Institute for Mathematics
Germany

Opponent

Professor Emmanuel Kowalski
ETH Zurich
Switzerland

ISBN 978-951-29-9304-8 (PRINT)
ISBN 978-951-29-9305-5 (PDF)
ISSN 0082-7002 (Print)
ISSN 2343-3175 (Online)
Painosalama, Turku, Finland, 2023

UNIVERSITY OF TURKU
Faculty of Science
Department of Mathematics and Statistics
Mathematics
JÄRVINIEMI, OLLI: Problems in analytic and algebraic number theory
Doctoral dissertation, 189 pp.
Doctoral programme in Exact Sciences (EXACTUS)
March 2023

ABSTRACT

In this thesis we study questions on the distribution of primes and multiplicative orders modulo prime numbers. The problems are attacked using methods from analytic and algebraic number theory.

In the first article, we consider the problem of finding primes in "many" short intervals. We improve on a result of Heath-Brown by combining his methods with Harman's sieve. We further extend the results for shorter intervals, considerably improving on a result of Peck. We give applications to prime-representing functions and binary digits of primes.

In the second article, together with J. Teräväinen, we study the distribution of Gaussian almost primes in narrow sectors, demonstrating that the previous results and methods of Teräväinen over the integers may be adapted to Gaussian integers. Our result for products of three Gaussian primes is almost optimal. The result for products of two Gaussian primes is of comparable strength as the best known results over integers.

In the third and fourth articles, we study multiplicative orders of integers modulo primes, motivated by Artin's primitive root conjecture. The results of these articles are conditional on a generalization of the Riemann hypothesis. In the third article, extending previous methods of Lenstra to a multivariable setting, we in particular determine all tuples of integers attaining equal orders modulo infinitely many primes. In the fourth article, together with A. Perucca, we unify many previous variations of Artin's conjecture into one framework, and give a finite procedure for solving such problems in general.

KEYWORDS: prime numbers, Dirichlet polynomials, Gaussian primes, Artin's conjecture

TURUN YLIOPISTO
Matemaattis-luonnontieteellinen tiedekunta
Matematiikan ja tilastotieteen laitos
Matematiikka
JÄRVINIEMI, OLLI: Problems in analytic and algebraic number theory
Väitöskirja, 189 s.
Eksaktien tieteiden tohtoriohjelma (EXACTUS)
Maaliskuu 2023

TIIVISTELMÄ

Tässä väitöskirjassa tutkitaan alkulukujen jakautumista ja multiplikatiivisia asteita modulo alkuluvut. Ongelmia lähestytään hyödyntämällä menetelmiä analyyttisestä ja algebrallisesta lukuteoriasta.

Ensimmäisessä artikkelissa tutkimme alkulukujen löytämistä "monilta" lyhyiltä väleiltä. Parannamme Heath-Brownin tulosta hyödyntämällä hänen menetelmiään ja Harmanin seulaa. Yleistämme tuloksia myös lyhyemmille väleille, parantaen huomattavasti Peckin tulosta. Tuloksille esitetään sovelluksia alkulukuja esittävistä funktioista ja alkulukujen binääriesityksistä.

Toisessa artikkelissa tutkimme yhdessä J. Teräväisen kanssa Gaussin melkein alkulukujen jakautumista kapeisiin sektoreihin. Demonstroimme, että Teräväisen tulokset ja menetelmät kokonaislukujen tapauksessa yleistyvät Gaussin kokonaislukujen tapaukseen. Tuloksemme kolmen Gaussin alkuluuvn tulolle on miltei paras mahdollinen. Kahden Gaussin alkuluvun tuloa koskeva tulos on vastaavan tasoinen kuin parhaat kokonaislukujen tapauksessa tunnetut tulokset.

Kolmannessa ja neljännessä artikkelissa tutkimme, Artinin primitiivijuurikonjektuurin innoittamana, kokonaislukujen multiplikatiivisia asteita modulo alkuluvut. Näiden artikkelien tulokset olettavat yleistetyn Riemannin hypoteesin. Kolmannessa artikkelissa yleistämme Lenstran menetelmiä monen muuttujan tapaukseen ja muun muassa määritämme kaikki kokonaislukutuplat, joiden multiplikatiiviset asteet ovat samat modulo äärettömän moni alkuluku. Neljännessä artikkelissa kokoamme yhdessä A. Peruccan kanssa monet aiemmin tutkitut muunnelmat Artinin konjektuurista yhteen kehykseen, ja esitämme äärellisen menetelmän tämän tyyppisten ongelmien ratkaisemiseksi.

ASIASANAT: alkuluvut, Dirichlet'n polynomit, Gaussin alkuluvut, Artinin konjektuuri

Acknowledgements

I am deeply grateful to my advisor, Prof. Kaisa Matomäki, for all the guidance she has offered during my PhD studies. The mathematical advice, detailed comments on my writings, and flexibility in practical matters have been an invaluable help. Certainly any expectations I had were met and exceeded.

Equally, I am deeply grateful to Joni Teräväinen for providing me mentorship, from when I had barely started my bachelor studies to commenting on drafts of this thesis, and being a valuable research collaborator. Our discussions and emails have immensely helped me grow as a mathematician.

I express my gratitude to Prof. Stephan Baier and Dr. Pieter Moree for serving as the reviewers of my thesis, and Prof. Emmanuel Kowalski for agreeing to act as the opponent at my defense.

I sincerely thank Prof. Antonella Perucca for arranging my visit to the University of Luxembourg and for the subsequent fruitful collaboration. I also thank the Emil Aaltonen foundation and Academy of Finland (grant no. 346307) for funding my doctoral studies.

I warmly thank my mother for raising me, for emphasizing the importance of education and encouraging me to pursue my interests.

Finally, I thank all of my friends from Päivölä and the math competition circles. I have learned so much from all of our discussions, be it on mathematics or other interests. It's been a lot of fun.

March 2023
Olli Järviniemi

Table of Contents

List of Original Publications

This dissertation is based on the following original publications, which are referred to in the text by their Roman numerals:

I O. Järviniemi. On large differences between consecutive primes. Preprint available at arXiv:2212.10965.

II O. Järviniemi and J. Teräväinen. Gaussian almost primes in almost all narrow sectors. Preprint available at arXiv:2303.05822.

III O. Järviniemi. Equality of orders of a set of integers modulo a prime. *Proc. Amer. Math. Soc. 149 (2021)*, no. 9, 3651–3668.

IV O. Järviniemi and A. Perucca. Unified treatment of Artin-type problems. *Res. Number Theory 9 (2023)*, no. 1, 10.

1 Notation

We introduce notation used in Sections 2 to 6.

1. **Sets.**
    - $\mathbb{N} = \{1, 2, 3, \ldots\}$ – natural numbers
    - $\mathbb{Z}$ – integers
    - $\mathbb{Q}$ – rational numbers
    - $\mathbb{R}$ – real numbers
    - $\mathbb{R}_+$ – positive real numbers
    - $\mathbb{C}$ – complex numbers
    - $\mathbb{P}$ – prime numbers
    - $\mathbb{Z}[i]$ – Gaussian integers
    - $\mathbb{P}_{\mathbb{Z}[i]}$ – Gaussian primes
    - K – number field
    - $K^\times$ – multiplicative group of non-zero elements of K
2. **Letters.**
    - p, q (possibly with subscripts) – prime numbers
    - ϵ – a small positive constant
    - W – a finitely generated multiplicative subgroup of $\mathbb{Q}^\times$
3. **Functions.**
    - $\pi(x)$ – number of primes not exceeding x
    - 1_A – indicator function of the set A
    - λ – the Liouville function
    - μ – the Möbius function
    - $\tau(n)$ – number of divisors of $n \in \mathbb{N}$
    - $\phi(m)$ – Euler phi function of m

- Re – real part of complex number
- Im – imaginary part of complex number
- N(n) – norm of $n \in \mathbb{Z}[i]$
- $\arg n$ – argument of $n \in \mathbb{Z}[i]$
- ord$_p(a)$ – multiplicative order of a modulo p
- Ind$_p(a)$ – the index of a modulo p, Ind$_p(a) = (p-1)/\text{ord}_p(a)$
- ord$_p(W)$ – size of the reduction of W modulo p
- Ind$_p(W)$ – the index of W modulo p, Ind$_p(W) = (p-1)/\text{ord}_p(W)$

4. **Number fields.**

- $K(\alpha_1, \dots, \alpha_n)$ – smallest extension of K containing $\alpha_1, \dots, \alpha_n$
- $[K : \mathbb{Q}]$ – degree of K over $\mathbb{Q}$
- ζ_n – the primitive nth root of unity $e^{2\pi i/n}$
- Gal$(K/\mathbb{Q})$ – Galois group of the extension $K/\mathbb{Q}$

5. **Asymptotics.**

- $f(x) = O(g(x))$ – there exists constant $C > 0$ such that $|f(x)| \leq Cg(x)$ for all sufficiently large x
- $f(x) \ll g(x)$ – shorthand for $f(x) = O(g(x))$
- $f(x) \gg g(x)$ – shorthand for $g(x) = O(f(x)), g(x) > 0$
- $f(x) = o(g(x))$ – shorthand for $\lim_{x\to\infty} |f(x)|/|g(x)| = 0$

6. **Miscellaneous**

- $\langle a_1, \dots, a_n \rangle$ – group generated by $a_1, \dots, a_n$
- $v_q(n)$ – q-adic valuation of n
- W_1W_2 – product $\{w_1w_2 | w_1 \in W_1, w_2 \in W_2\}$ of groups $W_1, W_2 \subset K^*$
- GRH – Generalized Riemann Hypothesis (see Hypothesis 5.4.1)

2 Introduction

Much of number theory revolves around prime numbers and in particular proving the existence of prime numbers with specific properties. The original articles of this thesis revolve around the following two questions and their variations.

***Question* 2.0.1.** *What can one say about the distribution of primes in short intervals?*

***Question* 2.0.2.** *What can one say about the order of* 2 *modulo* p*, as* p *ranges over the primes?*

We first focus on Question 2.0.1, with the following problem in our mind.

***Problem* 2.0.3** (Distribution of primes in short intervals)**.** *Given a function* $f : \mathbb{R}_+ \to \mathbb{R}_+$ *and large* X*, bound the number of integers* $x \in [X, 2X]$ *such that* $[x, x + f(X)]$ *contains no primes.*

It is known that that any interval of length $X^{0.525}$ contains primes, proven by Baker, Harman and Pintz [2]. This is far from what we expect to be true: Cramer's conjecture [4; 8] states that any interval of length $(\log X)^{2+\epsilon}$ contains primes for all large enough X in terms of ϵ. A natural barrier of current methods is intervals of length $\sqrt{X}$, as even under the Riemann hypothesis one can only show that intervals of length $C\sqrt{X}\log X$ contain primes for some constant $C > 0$ [48].

Hence, one often considers shorter intervals, but allows there to possibly be some exceptional values x such that there are no primes in $[x, x + f(X)]$. Jia [27] has shown that for $f(X) = X^{1/20+\epsilon}$ almost all such intervals contain primes. Again, this is far from what one would expect to be true, which is that the result holds for any f such that $f(X)/\log X \to \infty$ (see [18]). For intervals of length $\sqrt{X}$ Heath-Brown [22] has bounded the number of such x by $X^{3/5+\epsilon}$ for X large enough in terms of ϵ.

In Article I we improve on Heath-Brown's result, obtaining the bound $X^{0.57+\epsilon}$. This brings us closer to the bound $X^{1/2+\epsilon}$ following from the Riemann hypothesis [52]. The proof strategy is to combine Heath-Brown's recent methods [21; 22] with Harman's sieve. We further extend Heath-Brown's methods to intervals shorter than $\sqrt{X}$, namely by giving the bound $X^{0.63+\epsilon}$ for the number of intervals $[x, x + X^{0.45}]$ not containing primes, significantly improving on a result of Peck [38]. We give applications to prime-representing functions and primes with many ones in their binary representation.

Variants on questions on the distribution of primes are obtained by considering the distribution of almost primes.

***Problem* 2.0.4** (Distribution of almost primes in short intervals)**.** *Given a function $f : \mathbb{R}_+ \to \mathbb{R}_+$, integer $k \geq 2$ and large X, bound the number of integers $x \in [X, 2X]$ such that $[x, x + f(X)]$ contains no product of exactly k primes.*

The increased number of prime factors gives additional flexibility and allows one to show stronger results. Very recently, it has been shown by Matomäki and Teräväinen [33] that almost all intervals of length $(\log X)^{2.1}$ contain products of exactly two primes.

In Article II we consider the analogous problem in Gaussian integers, with short intervals replaced by narrow sectors. It is shown that, for X large enough, almost all sectors of a disk of radius $\sqrt{X}$ and of angular width $(\log X)^{15.1}/X$ contain products of exactly two Gaussian primes. This is achieved by generalizing previous results of Teräväinen [46] to the Gaussian setting. We show a corresponding result for products of three Gaussian primes in sectors of angular width $(\log X)^{1+\epsilon}/X, X \geq X_0(\epsilon)$, this result being almost optimal.

We then consider Question 2.0.2. A particularly important conjecture on multiplicative orders concerns the maximum possible value of orders modulo p.

***Conjecture* 2.0.5** (Artin's primitive root conjecture)**.** *Let $a \in \mathbb{Z} \setminus \{-1, 0, 1\}$ be given and assume a is not a square. There are infinitely many primes p such that* $\mathrm{ord}_p(a) = p - 1$.

Artin's conjecture is strongly supported by heuristic arguments and numerical results, indicating that, for any such a, the relative density (in the set of primes) of such primitive root producing p is strictly positive. Central milestones along the conjecture's nearly hundred year history include Hooley's [23] resolution under the Generalized Riemann Hypothesis (GRH) and Heath-Brown's [19] result that (in particular) Conjecture 2.0.5 is true for at least one of $a \in \{2, 3, 5\}$.

There are numerous variants of Artin's conjecture. To name a few, one could instead consider the primes p with $\mathrm{ord}_p(a) = (p-1)/h$ (near-primitive roots [35, Section 9.7.3]), conditions of form $\mathrm{ord}_p(a) = \mathrm{ord}_p(b) = p - 1$ (simultaneous primitive roots [34]), or the condition $\mathrm{ord}_p(b) \mid \mathrm{ord}_p(a)$ corresponding to solvability of $a^x \equiv b \pmod p$ (the two-variable Artin conjecture [36]).

Lenstra [29], building on works of Hooley [23] and Cooke–Weinberger [3], famously provided a systematic way for approaching such questions under GRH. In short, it suffices to check that any finite set of local valuation conditions (such as $v_2(\mathrm{ord}_p(a)) = v_2(p-1)$) on the orders may be simultaneously satisfied in order to obtain a global condition (such as $\mathrm{ord}_p(a) = p - 1$).

In Article III we generalize Lenstra's methods to a multivariable setting and, in particular, solve the Schinzel-Wójcik problem [42] on equality of orders under GRH.

***Problem* 2.0.6** (Schinzel-Wójcik)**.** *Determine all $a_1, \ldots, a_n \in \mathbb{Q}^\times$ such that there are infinitely many primes p with*

$$\mathrm{ord}_p(a_1) = \ldots = \mathrm{ord}_p(a_n).$$

The contents of the article and related topics are also covered in the author's master's thesis [26].

In Article IV we generalize the ideas further in a systematic way, giving a unified treatment of Artin-type problems. Indeed, many such questions may be seen as instances of the following general problem.

***Problem* 2.0.7** (Index map problem)**.** *Let $W_1, \ldots, W_n$ be finitely generated subgroups of $\mathbb{Q}^\times$. Describe the image of the index map*

$$p \mapsto (\mathrm{Ind}_p(W_1), \ldots, \mathrm{Ind}_p(W_n)) \tag{2.0.1}$$

as p ranges over the primes. Consider restricting to primes p satisfying a given Artin symbol condition, and consider the analogous problem over an arbitrary number field in place of $\mathbb{Q}$.

Under GRH, we give a satisfactory solution to Problem 2.0.7. In particular, we give an explicit finite procedure for computing the image of the index map. This provides a description of the image and a method for explicitly determining the image of the index in any given concrete case.

In the next four sections we give overviews of the ideas behind each of the articles. We aim to keep the exposition light, leaving the complete proofs and technical details to the articles.

3 On large differences between consecutive prime numbers

A central problem in number theory is understanding the distribution of primes. In particular, one may consider the number of primes in intervals: how many primes are there in $[1, x]$ or $[x, x + \sqrt{x}]$, or how long does an interval necessarily have to be for it to contain primes, what if one considers just almost all intervals, and so on.

In Article I we consider the problem of finding primes in "many" intervals of length $\sqrt{x}$ and $x^{0.45}$. Denoting by p_n the nth prime, we show the following.

***Theorem* 3.0.1.** *Let $x > 0$ be large enough. We have*

$$\sum_{\substack{p_n \in [x,2x] \\ p_{n+1}-p_n \geq x^{1/2}}} (p_{n+1} - p_n) \ll x^{0.57+\epsilon}$$

for any fixed $\epsilon > 0$.

***Theorem* 3.0.2.** *Let $x > 0$ be large enough. We have*

$$\sum_{\substack{p_n \in [x,2x] \\ p_{n+1}-p_n \geq x^{0.45}}} (p_{n+1} - p_n) \ll x^{0.63+\epsilon}$$

for any fixed $\epsilon > 0$.

Theorem 3.0.1 improves on a bound of Heath-Brown, who gave the estimate $x^{3/5+\epsilon}$. Previous results on the same problem have been given by Wolke with the exponent $29/30$ [50], Heath-Brown with $5/6+\epsilon$ [16], Heath-Brown again with $3/4+\epsilon$ [17], Peck with $25/36 + \epsilon$ [38] and Matomäki with $2/3$ [31]. The exponents are best viewed as $\frac{1}{2} + \delta$ with varying $\delta > 0$, since either the sum in Theorem 3.0.1 is empty or at least $x^{1/2}$, and standard conjectures such as the Lindelöf hypothesis or the Riemann hypothesis cannot rule out such large prime gaps.

In Theorem 3.0.2 the best previous result was given by Peck [39], resulting in the bound $x^{0.8+\epsilon}$. Here the exponents should be viewed as $0.55 + \delta$, as the Lindelöf hypothesis implies the bound $x^{0.55+\delta}$ for any $\delta > 0$ [52]. Our result's $\delta = 0.08 + \epsilon$ is less than a third of Peck's result's $\delta = 0.25 + \epsilon$. Peck's result, however, handles

intervals of any length, giving the bound $x^{1.25-c+\epsilon}$ for an interval of length x^c. Concurrently with our work, Stadlmann [44] improved Peck's result to $x^{1.23-c+\epsilon}$, though for intervals of length $x^{0.45}$ our result is stronger.

Below we outline some main ideas that are used in the proofs. A couple of central tools are complex analysis and *Dirichlet polynomials*. We start by a brief motivation on why exactly such tools are so useful to number theoretic problems on the distribution of primes. The author finds *pretentious number theory* (see [11; 9]) to give a particularly illuminating explanation for why one would consider Dirichlet polynomials in such problems. After this introduction we go into more detail about the methods we use for bounding the number of long prime gaps.

3.1 Why Dirichlet polynomials?

We take a slight detour from the distribution of prime numbers to the behavior of multiplicative functions. While these topics are superficially quite different, there turn out to be deep connections. Consider the following problem.

***Problem* 3.1.1** (Cancellation in multiplicative sums)**.** *Determine all multiplicative functions $f : \mathbb{N} \to \mathbb{C}$ for which $|f(n)| \leq 1$ and*

$$\lim_{x\to\infty} \frac{\sum_{n\leq x} f(n)}{x} = 0. \tag{3.1.1}$$

Perhaps the most natural example of a non-trivial 1-bounded multiplicative function is the Liouville function, defined by $\lambda(n) = 1$ if n has an even number of (not necessarily distinct) prime factors and $\lambda(n) = -1$ otherwise. A related example is the Möbius function $\mu(n) = \lambda(n)1_{n \text{ squarefree}}$. Intuition says that λ and μ are zero on average: certainly one would guess that 50% of positive integers have an even number of prime factors and 50% have an odd number, and that this would hold for squarefree numbers as well. However, proving this is not easy: it is well known (and not quite obvious) that the statement (3.1.1) for $f = \lambda$ (or $f = \mu$) is equivalent to the prime number theorem (see e.g. [1, Chapter 4]).

There are functions for which (3.1.1) does not hold. The most obvious example is $f \equiv 1$, but there are non-trivial examples as well. Namely, one can show that the function

$$f(n) = n^{it} = e^{it\log n}$$

does not satisfy (3.1.1) for any $t \in \mathbb{R}$. The reason is that the values $f(1), f(2), \dots$ circle around the unit circle with quickly shrinking step lengths, so that the points $f(1), f(2), \dots, f(\lfloor x \rfloor)$ are unevenly distributed on the unit circle. See Figure 1 for an illustration.

We note that one may obtain new counter-examples to (3.1.1) by modifying the above examples at some prime numbers: for example, the completely multiplicative

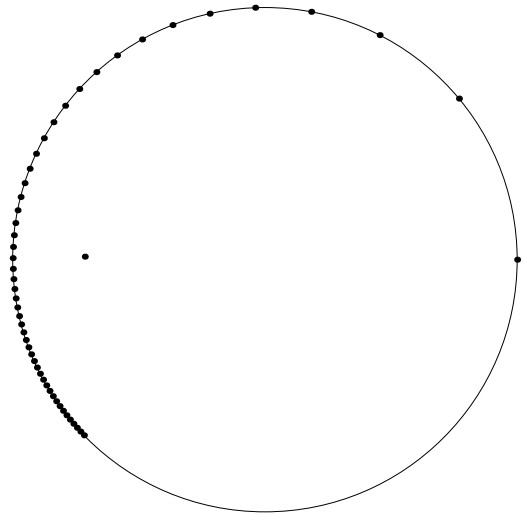

Figure 1. The points $n^{it} = e^{it \log n}$ for $t = 1$, $1 \leq n \leq 50$ and their average.

function f with $f(p) = 1/2$ for $p < 100$ and $f(p) = 1, p \geq 100$ does not satisfy (3.1.1) either.

The critical fact is that these are essentially the only counterexamples to (3.1.1). Namely, one can show that if f does not satisfy (3.1.1), then there is some $t \in \mathbb{R}$ such that $f(p)p^{-it}$ is roughly the constant function 1 – more precisely, the sum

$$\sum_{p \text{ prime}} \frac{1 - f(p)p^{-it}}{p}$$

is finite (this is Halász's theorem, see [12], [13], also [10]). In other words, $f(n)$ "pretends" to be the function n^{it}.

This demonstrates the general principle that in order to understand the averages of a sequence (a_n) (say $a_n = \lambda(n)$ or $a_n = 1_{n \text{ is prime}}$) in intervals, one should understand the sums

$$A(it) = \sum_{n \leq x} a_n n^{-it}$$

for various real numbers t. Indeed, the value $A(it)$ measures how strongly the sequence a_n behaves like the sequence n^{it}. Such functions $A(it)$ are called *Dirichlet polynomials*.

(We note that other ways to motivate the use of Dirichlet polynomials exist. For example, one sees that the functions $x \mapsto x^{it}$ are the characters of the group $(\mathbb{R}_+, \cdot)$, so any time one applies Fourier analysis one encounters the characters n^{it}.)

3.2 Reducing to Dirichlet polynomials

We then explain how in practice one reduces number-theoretic problems to ones on Dirichlet polynomials. The central tool is Perron's formula (see [25, Proposition 5.54]).

***Lemma* 3.2.1.** *Let (a_n) be a sequence of complex numbers and let $A(s) = \sum_{n\in\mathbb{N}} a_n n^{-s}$. Assume that $A(s)$ is absolutely convergent for $Re(s) > \sigma$. Then we have*

$$\sum_{n\leq x} a_n = \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} A(s)\frac{x^s}{s}\mathrm{d}s \qquad (3.2.1)$$

for any $c > \max(0,\sigma)$ and $x > 0$ (which is not an integer).

Note that by the lemma one can also access sums $\sum_{a<n\leq b} a_n$ over arbitrary intervals by replacing x^s with $b^s - a^s$ above.

Often one arranges things so that one wants to bound $\left|\sum_{n\leq x} a_n\right|$ from above by choosing the sequence a_n in a suitable way. For example, if one wants to bound the number of primes $p \leq x$, instead of $a_n = 1_{n \text{ prime}}$ one should choose something like $a_n = 1_{n \text{ prime}} - 1/\log n$, so that one expects $\sum_{n\leq x} a_n$ to be small.

The problem is then reduced to bounding the integral in (3.2.1). The integral is inconveniently over an infinite line. This technical issue is commonly resolved by using a truncated version of Perron's formula, where the integral is over $[c - iT, c + iT]$ for some large $T \in \mathbb{R}_+$.

In any case, one should not let the technicalities blur the main idea: the point is that the problem has been reduced to bounding the mean value of a Dirichlet polynomial. Indeed, we have

$$\left|\frac{1}{2\pi i}\int_{c-iT}^{c+iT} A(s)\frac{x^s}{s}\mathrm{d}s\right| \leq \int_{c-iT}^{c+iT} |A(s)|\frac{|x^s|}{|s|}\mathrm{d}|s| = x^c\int_{c-iT}^{c+iT} |A(s)|\frac{1}{|s|}\mathrm{d}|s|.$$

The term $1/|s|$ is also easy to control, as usually one performs a dyadic decomposition over the imaginary part of s. So the problem is essentially reduced to bounding

$$\int |A(it)|\mathrm{d}t.$$

However, in many cases a direct application of Perron's formula does not suffice. As mentioned above, one first normalizes the sequence a_n so that its average is expected to be small. Yet one also needs A to satisfy some additional properties. Most importantly, one wants A to factorize as the product of shorter polynomials – this will make the methods of bounding $A(it)$ work much better (or to work at all). We hence seek for choices which give more flexibility than the choice $a_n = 1_{n \text{ prime}} - 1/\log n$ presented above.

It is not easy to see how one could do better, though. Primes are, by their very nature, numbers which do not factorize. However, there are creative ways of working around this issue. Let us present a toy example which, while being a vast simplification of ideas that actually work, nevertheless conveys some intuition. One could try to count primes by writing

$$\begin{aligned}|\{p \le x : p \text{ prime}\}| = &|\{n \le x : n \text{ has at most two prime factors}\}| \\ &- |\{n \le x : n \text{ has exactly two prime factors}\}|.\end{aligned}$$

The integers n counted by the last term above by definition factorize into a product. Integers which are the product of at most two primes are not readily accessible. However, they are slightly more accessible by sieve methods than primes themselves, and this then leads to expressions that factorize. One can get more leverage by considering also numbers with exactly three prime factors and applying inclusion-exclusion.

In practice one applies more complicated identities than the one above, such as the identities of Heath-Brown [14, Section 2.5] and Buchstab [14, (1.4.13)] (which, at the end of the day, boil down to elementary combinatorics such as inclusion-exclusion). Often it is also sufficient to obtain merely lower bounds for the number of primes instead of an accurate asymptotic formula, which one can exploit by discarding some positive terms that could not be evaluated accurately. We employ an idea of this type, known as Harman's sieve, in our work.

3.3 Overview of the proof

We consider the specific task of showing that for "many" integers x there are primes in short intervals of the form $[x, x + \sqrt{x}]$ or $[x, x + x^{0.45}]$. In order to focus on the main ideas and keep things simple, some of the technical aspects are not represented accurately – we guide the interested reader to the original work.

The basic approach relies on Perron's formula in the form

$$\sum_{x<n\le x+y} a_n = \frac{1}{2\pi i}\int A(s)\frac{(x+y)^s - x^s}{s}\mathrm{d}s, \quad y \in \{x^{0.45}, x^{0.5}\}, \tag{3.3.1}$$

As explained in the previous section, we will not use the naive choice $a_n = 1_{n \text{ prime}}$ but something more complicated (explained below). In particular, we choose a_n so that one would expect $\sum a_n$ to be small.

We use a method due to Heath-Brown to exploit the fact that we do not need to consider $\sum a_n$ over all intervals $[x, x+y]$ but just "many" of them. The idea is that if there are many intervals $[x, x+y]$ such that the sum in (3.3.1) is unexpectedly large, one may add (with plus or minus signs) those sums together and obtain an expression of the form

$$\frac{1}{2\pi i}\int \frac{A(s)M(s)}{s}\mathrm{d}s$$

that is large, where $M(s)$ is a linear combination of terms of type z^s. Hence it suffices to obtain a good bound for this integral in order to bound the number of such exceptional intervals $[x, x+y]$. One should not pay attention to the $1/s$ factor: the problem is essentially to bound

$$\int |A(it)M(it)|\mathrm{d}t. \tag{3.3.2}$$

There are numerous tools one may use to bound mean values of Dirichlet polynomials (see [25, Chapter 9]). There are *large value theorems* of the form "the number of reals t for which $|A(it)| > V$ is at most $f(V)$". There are also *pointwise bounds* giving an upper bound for $|A(it)|$ that applies everywhere (corresponding to a large value theorem with $f(V) = 0$). Furthermore, there is a special tool applicable specifically for this problem: Heath-Brown [22, Proposition 1] has a mean value theorem that specifically allows one to bound integrals of the form $\int |P(it)M(it)|^2\mathrm{d}t$ with M as above. (This is slightly different from (3.3.2) due to the squaring in the integral.)

We arrange things so that $A(s)$ factorizes as a product of several polynomials, say $P_1(it)\cdots P_n(it)$. As is usual for bounding mean values, one then considers cases depending on how large $|P_j(it)|$ are for $1 \le j \le n$, as this allows one to apply the large value theorems above. Hence we fix some $V_1, \ldots, V_n$ and consider the integral

$$\int_{\mathcal{T}_{V_1,\ldots,V_n}} |P_1(it)\cdots P_n(it)M(it)|\mathrm{d}t$$

over the set $\mathcal{T}_{V_1,\ldots,V_n}$ of numbers t for which $|P_j(it)|$ is approximately V_j for all j.

One may think of the setup as a single-player game. We start from some initial position determined by the value of n, the lengths of the factors $P_j(\cdot)$ and the values $V_1, \ldots, V_n$. Our goal is to bound the integral above sufficiently well. Our allowed "moves" include applying large value theorems or pointwise bounds to some of the polynomials $P_j(\cdot)$ (or products or moments of such polynomials). There are also some special moves, such as Heath-Brown's mean value theorem. These require a bit of arrangement to work: to get a mean square as in Heath-Brown's theorem, one groups the factors $P_1(it)\cdots P_n(it)$ into two products $P(it)$ and $Q(it)$ and applies Cauchy-Schwarz to get

$$\int_{\mathcal{T}_{V_1,\ldots,V_n}} |P_1(it)\cdots P_n(it)M(it)|\mathrm{d}t \ll \sqrt{\int |P(it)M(it)|^2\mathrm{d}t}\sqrt{\int |Q(it)|^2\mathrm{d}t}.$$

The first integral is bounded by Heath-Brown's theorem, and for the second integral we use the "standard" moves based on large value theorems.

There are a lot of possible moves in the game and the set of initial positions is quite high-dimensional (and in particular infinite), making the game rather complex and difficult. The author wrote several programs to explore potential strategies in

order to play the game better, that is, to determine winning strategies when they exist. Of course, one cannot win every time: there are plenty of initial positions where a winning sequence of moves does not exist.

Having determined as many winnable initial positions as possible, we are left with representing the indicator $1_{n \text{ prime}}$ (or the corresponding polynomial $\sum p^{-it}$) in terms of sequences (a_n) whose corresponding polynomials $A(it)$ give winnable games. This problem is even more high-dimensional than the game played above. For this reason we rely on a computer search which shows that such a representation indeed exists. This part uses the Heath-Brown and Buchstab identities and Harman's sieve, with quite a lot of work needed to handle various technical issues.

We have now given a broad overview of the idea behind the proof. We guide the interested reader to the original article for the details.

4 Gaussian almost primes in almost all narrow sectors

Since many questions regarding primes themselves turn out to be very difficult, it is natural to consider analogous questions in easier setups. One such setup is considering almost primes, namely numbers that are products of just a few primes. More precisely, we let E_k denote the set of positive integers which are the product of *exactly* k primes. (It is also common to consider numbers which are the product of *at most* k primes. They turn out to be easier, as one may employ classical sieve methods, but this is another story.) Note that E_1-numbers are exactly the primes.

As with primes, one may consider the distribution of E_k-numbers in short intervals. The methods employed are quite similar (cf. Section 3): again it is natural to consider Dirichlet polynomials and use Perron's formula, and again one may use the large value theorems and pointwise bounds for polynomials. However, there is one crucial difference. For primes, it requires work to get the relevant Dirichlet polynomials to factorize, whereas for E_k-numbers one, by definition, necessarily has factorization. This makes E_k-numbers easier to work with and one obtains significantly stronger results.

Teräväinen [46] has shown that almost all intervals $[x, x + (\log x)^{3.51}]$ contain E_2-numbers and that almost all intervals $[x, x + (\log x)(\log\log x)^{6+\epsilon}]$ contain E_3-numbers. The result for E_2-numbers was very recently improved by Matomäki and Teräväinen [33] to intervals of length $(\log x)^{2.1}$ (interestingly, using the same mean value theorem of Heath-Brown as we use in Article I).

We set out to give analogous results for Gaussian integers. Namely, we show the following results.

***Theorem* 4.0.1.** *Let X be large and let $h = (\log X)^{15.1}$. Almost all sectors $\{n \in \mathbb{Z}[i], \mathrm{N}(n) \leq X : \theta \leq \arg n < \theta + \frac{h}{X}\}$ contain a product of exactly two Gaussian primes.*

***Theorem* 4.0.2.** *Let X be large and $h = (\log X)(\log\log X)^{19.2}$. Almost all sectors $\{n \in \mathbb{Z}[i], \mathrm{N}(n) \leq X : \theta \leq \arg n < \theta + \frac{h}{X}\}$ contain a product of exactly three Gaussian primes.*

Here "almost all" means that the Lebesgue measure of θ not satisfying the condition approaches zero as X tends to infinity. One thus sees that Theorems 4.0.1 and

4.0.2 give bounds which are qualitatively of the same strength as the best results over the integers.

Below we give a short indication of how one may approach the problems for E_k-numbers, highlighting a connection to the famous Matomäki–Radziwiłł method [32]. We then give a quick refresh on Gaussian integers, after which we discuss how the methods can be adapted to this setting, indicating some challenges that one faces in the process.

4.1 Almost primes

Consider first the case of E_2-numbers, with the aim of finding them in almost all intervals of form $[x, x+y]$. First, since we only have to find some E_2-numbers in an interval, it suffices to consider only specific E_2-numbers. This allows us to choose the sizes of the factors. Hence, choose some parameter z, and let $a_n = 1$ if $n = pq$, where p and q are primes with $q \approx z$. Then applying Perron's formula we have

$$\sum_{x<n\leq x+y} a_n = \frac{1}{2\pi i}\int A(s)\frac{(x+y)^s - x^s}{s}\mathrm{d}s.$$

The Dirichlet polynomial $A(s)$ essentially factorizes into the product of

$$Q(s) = \sum_{q\approx z} q^{-s} \quad \text{and} \quad P(s) = \sum_{p\approx x/z} p^{-s}$$

(after some technical arrangements). In contrast to the situation in Chapter 3, we may choose the lengths of the factors $Q(s)$ and $P(s)$. A good choice turns out to be $z = (\log x)^c$ for some constant c (so that $Q(s)$ is rather short).

Once again the problem reduces to bounding a mean value of Dirichlet polynomials, this time of the form

$$\int |A(s)|^2 \mathrm{d}|s| = \int |P(s)Q(s)|^2 \mathrm{d}|s|.$$

The way the problem is reduced to Dirichlet polynomials is different from Chapter 3, though, and hence we have a mean square here and there is no polynomial $M(s)$ this time. The methods again include large value theorems, mean value theorems and pointwise bounds and dividing the integral into pieces depending on the sizes of $|P(s)|$ and $|Q(s)|$. Furthermore, the polynomial $P(s)$ corresponds to a sum over primes, and so just as before we may use various identities to make the polynomial $P(s)$ factorize. We do note, however, that the actual large and mean value theorems used are somewhat different from those in Chapter 3 and the polynomial $Q(s)$ is much shorter than the polynomials there, and hence the proof requires different ideas.

It is now clear that for larger values of k the E_k-numbers are easier to control: the Dirichlet polynomial $A(s)$ factorizes as k polynomials, whose lengths we can

choose, and more factors give more flexibility. Indeed, the best known results are the stronger the larger k is.

We note that the work of Teräväinen on E_k-numbers builds on the Matomäki–Radziwiłł method. In their seminal work, Matomäki and Radziwiłł [32] (see also [43]) considered the averages of multiplicative functions in short intervals and in particular showed that the Liouville function $\lambda(n)$ has a small average on almost all intervals $[x, x+y]$ for any function y tending to infinity with x. Compare this to primes, for which we can only access intervals of length $y = x^c$ (we have lower bounds when $c > 1/20$ [27] and asymptotics when $c \geq 1/6$ [53]).

The reason multiplicative functions work so much better than primes or even the E_k numbers is that one immediately has an unbounded amount of factors. Let us explain. Almost all integers have a factor which is close to, say, $\log x$ (more precisely, a factor in $[\log x, (\log x)^{\Psi(x)}]$ for any $\Psi(x)$ tending to infinity), so that one may write almost all integers $n \approx x$ as $m_1 m_2$, where $m_1 \approx \log x$ and $m_2 \approx x/\log x$. By multiplicativity we have $\lambda(n) = \lambda(m_1)\lambda(m_2)$. This allows one to factorize the polynomial $A(s) = \sum \lambda(n) n^{-s}$ essentially as a product $M_1(s)M_2(s)$, where

$$M_1(s) = \sum_{m_1 \approx \log x} \lambda(m_1) m_1^{-s} \quad \text{and} \quad M_2(s) = \sum_{m_2 \approx x/\log x} \lambda(m_2) m_2^{-s}.$$

Nothing stops one from factorizing $M_1(s)$ and $M_2(s)$ in the same manner as $A(s)$. Hence, one can choose the number and lengths of factors of $A(s)$ in more or less any way one desires. (Needless to say, this sketch misrepresents many technical details. In practice one takes m_1 to be a prime, one has to be careful to not double-count integers n representable as $m_1 m_2$ in more than one way, and the approximations above should be made precise.)

While E_k-numbers are not quite as malleable as multiplicative functions, nevertheless the spirit carries over. And indeed, as k grows larger one can find E_k-numbers in intervals whose length approaches $\log x$ [46], an almost optimal result and a natural barrier for current methods.

4.2 The Gaussian integers

Recall that the *Gaussian integers* $\mathbb{Z}[i]$ are numbers of the form $a + bi$, where $a, b \in \mathbb{Z}$. Equipped with the usual addition and multiplication of complex numbers they form an interesting variant of the ordinary integers $\mathbb{Z}$. In particular, one may define *Gaussian primes* as numbers $z \in \mathbb{Z}[i]$ which cannot be written in a non-trivial way as the product of two Gaussian integers (non-trivial meaning that neither of the factors is one of the units $1, i, -1$ or $-i$). As with the integers, any Gaussian integer is the product of Gaussian primes in an unique way (if one neglects factors of $1, i, -1, -i$).

One may then consider variants of problems adapted to the Gaussian setting. For example, one may consider the distribution of Gaussian primes, or Gaussian almost

primes, or study the behavior of multiplicative functions in Gaussian integers.

There are several ways one may generate such variants. For example, if one sets to find Gaussian primes, one could try to find Gaussian primes which are a certain distance away from the origin (ordering Gaussian integers by their *norm*), which are at a certain angle viewed from the origin (ordering Gaussian integers by their *argument*), or asking how large a circle or square in the plane has to be to necessarily contain Gaussian primes (which corresponds to considering both norm and argument).

It turns out that many problems where one orders Gaussian integers by norm reduce to analogous problems on the integers. For example, finding Gaussian primes with norm in $[x, x+y]$ corresponds to finding ordinary primes p with $p \equiv 1 \pmod 4$ in $[x, x+y]$, or questions on averages of multiplicative functions on Gaussian integers with norm lying in $[x, x+y]$ are directly reduced to such problems on integers.

Ordering Gaussian integers by their argument, however, leads to new and interesting problems. We demonstrate that the Matomäki–Radziwiłł method may be adapted to this setting. Hence, while we consider the particular problem of finding E_k-numbers (or rather their Gaussian analogues) in narrow sectors, the methods generalize to questions on multiplicative functions.

We mention some previous work on Gaussian primes in narrow sectors and small circles. For sectors, it is known that sectors of the circle of radius $\sqrt{X}$ with area $X^{0.619}$ [15] contain Gaussian primes, with asymptotic formulas valid for sectors of area $X^{7/10+\epsilon}$ [41] (compare this to integers, with the corresponding bounds $X^{0.525}$ [2] and $X^{7/12}$ [20]). Relaxing to almost all sectors, one has asymptotics for sectors of area $X^{2/5+\epsilon}$ [24] (in integers the corresponding bound is $X^{1/6}$ [53]). For small circles, in turn, one can find Gaussian primes within a radius of $O(|z|^{0.528})$ from any point z [30]. See [14, Chapter 11] for more references.

One sees that the problem of finding Gaussian primes in small circles is easier than for narrow sectors (as one obtains better bounds). We indeed believe that our results for narrow sectors may be adapted to small circles as well.

4.3 Adapting to Gaussian integers

The Dirichlet polynomials $A(it) = \sum_{n \le x} a_n n^{-it}$ measure how closely (a_n) behaves like n^{it}, which is relevant when studying the behavior of the sequence (a_n) in short intervals. However, as now we are interested in sectors instead of intervals, the Dirichlet polynomials are no longer the right tool for the task. Instead, we consider *Hecke polynomials*

$$A(m) = \sum_{\mathrm{N}(n) \le x} a_n \lambda^{-m}(n), \quad \lambda^m(n) := \left(\frac{n}{|n|}\right)^{4m}, m \in \mathbb{Z}$$

to study the distribution of $a_n, n \in \mathbb{Z}[i]$. Here $\lambda^m(n)$ is a *Hecke character*, serving a similar purpose as the *Archimedean character* n^{it} serves when studying the distribution of numbers in intervals. Note that $n/|n|$ is a complex number on the unit circle at angle $\arg(n)$. The 4 in the exponent is there for symmetry, so that we have $\lambda^m(n) = \lambda^m(un)$ for any $u \in \{1, i, -1, -i\}$.

In Chapter 3.1 the use of Archimedean characters was motivated through studying the averages of multiplicative functions. One could give a similar motivation for Hecke characters. Consider whether a multiplicative function $f : \mathbb{Z}[i] \setminus \{0\} \to \mathbb{C}$ satisfies

$$\lim_{x\to\infty} \frac{1}{x} \sum_{\substack{\mathrm{N}(n)\leq x \\ \alpha<\arg(n)\leq\beta}} f(n) = 0 \tag{4.3.1}$$

for any fixed $0 \leq \alpha < \beta \leq 2\pi$. One family of counter-examples to (4.3.1) is $f(n) = \mathrm{N}(n)^{it}$, imitating the counter-example for the analogous problem on the integers. However, there is another such family, namely $f(n) = (n/|n|)^m$ for any integer m – indeed, in this case $f(n)$ is roughly constant in any fixed small sector. And so, as with short intervals and Dirichlet polynomials, in general the study of distribution of a sequence in narrow sectors is best done via Hecke polynomials. (And again another motivation could be given by noting that the functions $\lambda^m(n)$ are characters of $(\mathbb{C}\setminus\{0\}, \cdot)$, so that the Hecke characters arise when performing Fourier analysis.)

Perron's formula is no longer quite the right tool, but as before the problem is reduced to considering character sums and thus we it suffices to consider mean values of Hecke polynomials. Many of the large value theorems, mean value theorems and pointwise bounds carry over to Hecke polynomials with analogous proofs.

Nevertheless, there are a couple of result for which no analogue for Hecke polynomials is known. A major reason is the lack of understanding of the Hecke zeta functions

$$\zeta(s, \lambda^m) = \frac{1}{4} \sum_{n\in\mathbb{Z}[i]\setminus\{0\}} \frac{\lambda^m(n)}{\mathrm{N}(n)^s}$$

(where we divide by 4 due to the symmetry caused by $1, i, -1, -i$) when compared to the Riemann zeta function

$$\zeta(s) = \sum_{n\in\mathbb{N}} \frac{1}{n^s}.$$

For example, the fourth moment of the Riemann zeta function is known (see e.g. [47, Chapter 7.6]), whereas the fourth moment of the Hecke zeta functions is not. In terms of Dirichlet / Hecke polynomials this means that we have essentially optimal (upper) bounds for

$$\int |D(it)|^4 \mathrm{d}t$$

for a Dirichlet polynomial $D(it)$ of the form $D(it) = \sum_{d \le x} d^{-it}$, but the corresponding bound is not known for

$$\sum |H(m)|^4$$

for a Hecke polynomial $H(m) = \sum_{\mathrm{N}(n) \le x} \lambda^m(n)$. Similarly, the best pointwise bounds for $|H(m)|$ are worse than for $|D(it)|$, as we have worse pointwise bounds for the Hecke zeta function.

We cannot do anything about the lack of fourth moment estimates. However, we can obtain pointwise bounds via other means. Namely, we interpret $\sum_{\mathrm{N}(n) \le x} \lambda^m(n)$ as an exponential sum by writing

$$\sum_{\mathrm{N}(n) \le x} \lambda^m(n) = \sum_{\substack{a,b \in \mathbb{Z} \\ a^2+b^2 \le x}} e\left(4m \arctan\left(\frac{b}{a}\right)\right).$$

Sums of form $\sum_{n \le x} e(f(n))$ may be bounded by the theory of exponential pairs [7]. By chopping up the sum above to one-dimensional sums over a or b we then get upper bounds for $\sum_{\mathrm{N}(n) \le x} \lambda^m(n)$, which allows us to salvage versions of the respective mean and large value theorems.

Another central difficulty is bounding certain terms appearing in the mean and large value theorems. More specifically, in the integer case there is a mean value theorem of the form

$$\int_{-T}^{T} |A(it)|^2 \mathrm{d}t \ll T \sum_{\substack{n,m \le x \\ |n-m| \le x/T}} |a_n a_m|,$$

where $A(s) = \sum_{n \le x} a_n n^{-s}$. For example, if $a_n = 1_{n \text{ prime}}$, this results in having to bound from above the number of primes in intervals of length x/T from above. This is a rather standard sieve-theoretic problem. However, in the case of Gaussian integers the corresponding theorem gives

$$\sum_{t=1}^{T} |A(t)|^2 \ll T \sum_{\substack{\mathrm{N}(n),\mathrm{N}(m) \le x \\ |\arg n - \arg m| \le 1/T}} |a_n a_m|,$$

where $A(t) = \sum_{\mathrm{N}(n) \le x} a_n \lambda^m(n)$. For $a_n = 1_{n \in \mathbb{P}_{\mathbb{Z}[i]}}$ one thus has to bound the number of Gaussian primes in sectors of angular width $1/T$, which is not a standard problem.

This problem is solved as follows: If $\arg n \approx \arg m$, the imaginary part of $\overline{n}m$ is small. Hence, writing $n = a + bi, m = c + di$ one has (roughly) $|\mathrm{Im}(\overline{n}m)| =$

$|ad-bc| \leq x/T$. Thus we have, more or less,

$$\sum_{\substack{n,m\in\mathbb{P}_{\mathbb{Z}[i]}\\ \mathrm{N}(n),\mathrm{N}(m)\leq x\\ |\arg n-\arg m|\leq 1/T}} 1 \ll \sum_{0\leq k\leq x/T} \sum_{\substack{a,b,c,d\leq\sqrt{x}\\ ad-bc=k}} 1_{a+bi\in\mathbb{P}_{\mathbb{Z}[i]}} 1_{c+di\in\mathbb{P}_{\mathbb{Z}[i]}}$$

$$\approx \sum_{0\leq k\leq x/T} \sum_{\substack{a,b,c,d\leq\sqrt{x}\\ ad-bc=k}} 1_{a^2+b^2\in\mathbb{P}} 1_{c^2+d^2\in\mathbb{P}}.$$

By sieve methods we may upper bound the number of primes in a set if we understand well enough the number of integers in the set divisible by T for any $T \leq x^{\epsilon}$. Thus, we wish to asymptotically evaluate, for various T_1, T_2,

$$\sum_{\substack{a,b,c,d\leq\sqrt{X}\\ ad-bc=k\\ T_1|a^2+b^2\\ T_2|c^2+d^2}} 1.$$

This is in spirit the same sum as

$$\sum_{\substack{a,b,c,d\in\mathbb{N}\\ bc\leq X\\ ad-bc=k}} 1 = \sum_{n\leq X} \tau(n)\tau(n+k)$$

with additional congruence conditions on a, b, c, d with relatively small moduli. The sum over $\tau(n)\tau(n+k)$ is well understood (see [5]), and the methods used to treat that sum adapt to our case as well.

We have now given an overview of some fundamental ideas and tools behind our work. We refer the reader to the article for details.

5 Equality of orders of a set of integers modulo a prime

There is plenty of literature on Artin's primitive root conjecture and its variants. Below we give an exposition of the conjecture, giving a heuristic approach and then discussing the details and technical challenges. After that we will move on to the so-called Schinzel–Wójcik problem on equality of orders of integers, whose (GRH-conditional) resolution is our main result.

***Theorem* 5.0.1.** *Assume GRH. Given $a_1, \ldots, a_n \in \mathbb{Q}^\times \setminus \{-1, 1\}$, there are infinitely many primes p such that*

$$\mathrm{ord}_p(a_1) = \ldots = \mathrm{ord}_p(a_n)$$

if and only if at least one of the following statements is false:

1. *There exist integers e_i such that*

$$\prod a_i^{e_i} = -1.$$

2. *There exist integers f_i with an odd sum such that*

$$\prod a_i^{f_i} = 1.$$

As will become clear in the course of our exposition, the underlying methods adapt to a large class of problems regarding orders of integers modulo primes.

5.1 Heuristic argument

The famous Artin conjecture states the following.

***Conjecture* 5.1.1** (Artin's primitive root conjecture)**.** *Let $a \in \mathbb{Q}^\times \setminus \{-1, 1\}$ be given and assume a is not a square. There are infinitely many primes p such that* $\mathrm{ord}_p(a) = p - 1$.

(Note that while $\mathrm{ord}_p(a)$ is often defined only for $a \in \mathbb{Z}$, one may extend the definition to rationals by straightforward means.)

It is well known that for any p there exists a primitive root g modulo p, so that the multiplicative group of non-zero integers modulo p is cyclic and generated by g. One then sees that the perfect (non-zero) squares modulo p are exactly $\{g^k : 2 \mid k\}$, perfect cubes are $\{g^k : 3 \mid k\}$ and so on. If, for example, $3 \nmid p-1$, then clearly any element mod p is a cube. These ideas yield the following lemma.

***Lemma* 5.1.2.** *Let a be an integer modulo p. Then a is a primitive root modulo p if and only if, for any prime $q \mid p-1$, a is not a qth power modulo p.*

Motivated by this, for a prime q let $C_q = C_{q,a}(p)$ denote the condition

$$p \equiv 1 \pmod{q} \text{ and } a \text{ is a } q\text{th power modulo } p.$$

We are thus interested in finding primes p such that none of the conditions C_q are satisfied.

For the heuristic argument, it will be convenient to use probabilistic language, and hence we let E_q denote the event that a "random" prime p satisfies the condition C_q. As our purpose is to merely sketch a heuristic idea, we will not make these notions of probability and randomness rigorous, but rather rely on an intuitive notion of a random prime.

We first consider just a single prime q and the corresponding condition C_q. The condition consists of two parts: imposing that $p \equiv 1 \pmod{q}$, and then imposing that a is a qth power modulo p. For a prime $p \neq q$, there are $q-1$ possible values for $p \pmod{q}$, and one thus guesses that $p \equiv 1 \pmod{q}$ is satisfied for a proportion of $1/(q-1)$ of primes p. There are precise results of this form, most notably the prime number theorem in arithmetic progressions.

The power residue condition is more difficult to handle. One could guess that since $(p-1)/q$ of the $p-1$ non-zero elements modulo p are qth powers, the probability of a being a qth power is $1/q$. Clearly this heuristic fails if a is a qth power of a rational number, but otherwise this guess seems reasonable.

Put together we guess that the probability of E_q is

$$P(E_q) \stackrel{?}{=} \frac{1}{(q-1)q}, \tag{5.1.1}$$

at least if a is not a perfect power.

There is another heuristic in addition to (5.1.1) that we employ. One could guess that the information "a is a cube modulo p" does not tell much one way or another about if a is a fifth power modulo p or not. More generally, one could guess that the conditions C_q are independent of each other, so that

$$P\left(\bigcap_{i=1}^{n} E_{q_i}^c\right) \stackrel{?}{=} \prod_{i=1}^{n} P(E_{q_i}^c), \tag{5.1.2}$$

where E^c denotes the complement of the event E.

We can now make a reasonable heuristic concerning the set of primes p which satisfy none of the conditions C_q. Hoping that the independence heuristic (5.1.2) extends to infinitely many conditions, one has

$$P\left(\left(\bigcup_{q \text{ prime}} E_q\right)^c\right) = P\left(\bigcap_{q \text{ prime}} E_q^c\right) \stackrel{?}{=} \prod_{q \text{ prime}} P(E_q^c) \stackrel{?}{=} \prod_{q \text{ prime}} \left(1 - \frac{1}{(q-1)q}\right). \tag{5.1.3}$$

The final product is known as Artin's constant, and is numerically

$$A = \prod_{q \text{ prime}} \left(1 - \frac{1}{q(q-1)}\right) \approx 0.374, \tag{5.1.4}$$

a strictly positive constant.

We note that the heuristic holds up well for $a = 2$ (resp. $a = 3$): out of the first $10\,000$ primes coprime to a, 3750 (resp. 3771) are such that 2 (resp. 3) is a primitive root modulo p. Of course, for the perfect powers $a = 4$ and $a = 8$ the heuristic (5.1.1) fails (there are 0 and 2248 such primes p, respectively), and in the more subtle case $a = 5$ the independence assumption fails (there are 3959 such primes).

5.2 Rigorous approach

Making this heuristic argument formal requires two ingredients. First, while the heuristic guesses (5.1.1) and (5.1.2) are roughly correct, there are, as noted above, certain cases where they fail. Second, care is needed when considering infinitely many conditions C_q at once. Let us first consider the latter problem.

Still in heuristic mode, the idea is that the probabilities $P(E_q)$ decay quadratically in q (at least if (5.1.1) is true), and hence the probability of some of the events E_q with q "large" occurring should be "small". Indeed, we have, for any constant k,

$$P\left(\bigcup_{q>k} E_q\right) \leq \sum_{q>k} P(E_q) \stackrel{?}{=} \sum_{q>k} \frac{1}{(q-1)q},$$

the right hand side tending to zero as k tends to infinity.

Taking a more rigorous stance, one believes that the quantities

$$c_k := \limsup_{x \to \infty} \frac{|\{p \leq x : \exists q > k \text{ s.t. } p \text{ satisfies } C_q\}|}{|\{p \leq x : p \text{ prime}\}|} \tag{5.2.1}$$

tend to 0 as $k \to \infty$:

$$\lim_{k\to\infty} c_k \stackrel{?}{=} 0. \tag{5.2.2}$$

Assuming (5.2.2), one can reduce Artin's conjecture to considering merely finitely many conditions C_q, as we have

$$\begin{aligned}&|\{p \le x : a \text{ is a primitive root mod } p\}| = \\ &|\{p \le x : p \text{ does not satisfy } C_q \text{ for any } q \le k\}| + O(\pi(x)c_k)\end{aligned}$$

(the implied constant in the O-term being bounded by 1), and hence taking k large enough the error term is negligible. This brings us back to the heuristics (5.1.1) and (5.1.2), which hint that

$$\lim_{x\to\infty} \frac{|\{p \le x : p \text{ does not satisfy } C_q \text{ for any } q \le k\}|}{\pi(x)} \stackrel{?}{=} \prod_{q\le k}\left(1 - \frac{1}{(q-1)q}\right) \tag{5.2.3}$$

is true (at least for generic values of a, such as $a = 2$). If true, this then implies Artin's conjecture, with the density of primitive root producing primes p being given by Artin's constant (5.1.4).

Proving (5.2.2) is precisely the difficult part of Artin's conjecture: (5.2.2) is not known unconditionally. This is the analytic part of Artin's conjecture. Formalizing the heuristics (5.1.1) and (5.1.2), and also determining the possible corrections needed to the formulas, may be done unconditionally, this forming the algebraic side of the conjecture. We first consider the algebraic side, then the analytic side.

5.3 Algebraic methods

The problem at hand is computing, for any fixed n and distinct primes $q_1, \dots, q_n$, (informally) the probability $P(E_{q_1} \cap \ldots \cap E_{q_k})$ or (formally) the density

$$\lim_{x\to\infty} \frac{|\{p \le x : p \text{ satisfies } C_{q_i} \text{ for } 1 \le i \le n\}|}{\pi(x)}.$$

The left hand side of (5.2.3) could then be computed by inclusion-exclusion.

Writing $m = q_1 \cdots q_n$, note that p satisfies C_{q_i} for $1 \le i \le n$ if and only if $p \equiv 1 \pmod m$ and a is an mth power modulo p. Hence, we wish to compute

$$\lim_{x\to\infty} \frac{|\{p \le x : p \equiv 1 \pmod m \text{ and } a \text{ is an } m\text{th power modulo } p\}|}{\pi(x)}.$$

As mentioned before, the congruence condition is rather easy to tackle: namely, the prime number theorem on arithmetic progressions states

$$\lim_{x\to\infty} \frac{|\{p \le x : p \equiv 1 \pmod m\}|}{\pi(x)} = \frac{1}{\phi(m)}.$$

The power residue condition is more difficult. For $m = 2$ one could appeal to the law of quadratic reciprocity, but this method does not generalize.

It is a very non-obvious and deep idea, which we cannot do justice here, that power residue (and other similar) conditions are best viewed through the theory of field extensions. The celebrated Chebotarev density theorem (see e.g. [45]) provides one reason why, giving a formula for the number of primes p satisfying such conditions, with the formula depending on the properties of relevant field extensions. As the theorem is somewhat technical, in this exposition we stick to the following simple consequence.

***Lemma* 5.3.1** (Consequence of the Chebotarev density theorem)**.** *For any $m \in \mathbb{N}$ we have*

$$\lim_{x\to\infty} \frac{|\{p \leq x : p \equiv 1 \pmod m, a \text{ is an } m\text{th power mod } p\}|}{\pi(x)} = \frac{1}{[\mathbb{Q}(\zeta_m, a^{1/m}) : \mathbb{Q}]}.$$

Recall that here $[K : \mathbb{Q}]$ denotes the degree of K over $\mathbb{Q}$.

The question then reduces to computing the degree of the field $\mathbb{Q}(\zeta_m, a^{1/m})$ over $\mathbb{Q}$. The root of unity ζ_m has degree $\phi(m)$ over $\mathbb{Q}$. Furthermore, $a^{1/m}$ has degree at most m over $\mathbb{Q}$, as $a^{1/m}$ is a root of the polynomial $X^m - a$. This shows that $\phi(m)m$ is an upper bound for the degree. The heuristics (5.1.1) and (5.1.2) correspond to asking that equality holds for any square-free m.

In order to compute the degrees $[\mathbb{Q}(\zeta_m, a^{1/m}) : \mathbb{Q}]$, it is instructive to consider reasons for why the upper bound may not be attained. We have already mentioned one, namely that a may be a perfect power. Another, more subtle reason is that square root of integers lie in cyclotomic fields. For example, one has

$$\begin{aligned}
\sqrt{2} &= \zeta_8 + \zeta_8^{-1} \in \mathbb{Q}(\zeta_8), \\
\sqrt{3} &= i(\zeta_3 - \zeta_3^2) \in \mathbb{Q}(\zeta_{12}), \quad \text{and} \\
\sqrt{5} &= \zeta_5 - \zeta_5^2 - \zeta_5^3 + \zeta_5^4 \in \mathbb{Q}(\zeta_5).
\end{aligned}$$

In elementary terms, quadratic residue information and congruence information are not independent of each other, as is demonstrated by the law of quadratic reciprocity (which, by the way, is naturally viewed in terms of field theory). This causes the independency assumption (5.1.2) to fail in certain cases.

These two reasons turn out to be the *only* reasons for the failure of maximality of extensions of form $\mathbb{Q}(\zeta_m, a^{1/m})$ (we omit the proof). From here one may easily compute the degrees. For example, if a is not a perfect power, then $[\mathbb{Q}(\zeta_m, a^{1/m}) : \mathbb{Q}] = m\phi(m)$, except if m is even and $\sqrt{a} \in \mathbb{Q}(\zeta_m)$, in which case we have $[\mathbb{Q}(\zeta_m, a^{1/m}) : \mathbb{Q}] = m\phi(m)/2$. Furthermore, the set of m for which $\sqrt{a} \in \mathbb{Q}(\zeta_m)$ is the set of integers divisible by an integer m_a, where one may describe m_a explicitly in terms of the prime factorization of a. With these ideas one can compute the left hand side of (5.2.3), although the general case requires a bit of calculation.

5.4 Analytic methods

The analytic argument goes back to Hooley [23], see also [6, Theorem 4] and [49, Theorem 5.1]. The version of GRH we will be using is as follows (see [23], [28]).

***Hypothesis* 5.4.1** (Generalized Riemann Hypothesis)**.** *For any number field K, the non-trivial zeros of the Dedekind zeta function of K lie on the line Re$(s) = \frac{1}{2}$.*

(In fact, it would be sufficient to assume GRH only for the number fields used in the proof.)

Our task is to show (5.2.2) (conditionally on GRH). Depending on the size of q we employ different methods for showing that $|\{p \le x : p \text{ satisfies } C_q\}|$ is small.

A natural idea is to apply versions of Lemma 5.3.1 with effective error terms. The error terms are of same strength as for the usual prime number theorem: unconditionally one does not have any power-saving error term and thus does not get very far, but conditionally on a suitable Riemann hypothesis one has roughly square-root error terms. This alone allows one to handle q smaller than (roughly) $\sqrt{x}$. In more detail, GRH implies that

$$|\{p \le x : p \text{ satisfies } C_q\}| = \frac{\pi(x)}{[\mathbb{Q}(\zeta_q, a^{1/q}) : \mathbb{Q}]} + O(\sqrt{x}(\log x)^B)$$

for some constant B (see [28]). Summing up the main term for all primes $q > k$ would lead to an acceptable contribution, but the error term allows one to only consider q smaller than $\sqrt{x}/(\log x)^{B+2}$ or so.

How about very large values of q? Noting that C_q being satisfied implies that $\mathrm{ord}_p(a) \le (p-1)/q$, it follows that $\mathrm{ord}_p(a)$ is then very small. If q is very large, say $q \approx x/100$, one would have $\mathrm{ord}_p(a) \le 100$ and thus $p \le a^{100} = O(1)$, which is not possible for p large enough. For slightly smaller values of q there could be some primes p with $\mathrm{ord}_p(a)$ smaller than $(p-1)/q$, but this would be exceptional: p would then have to divide a number of form $a^n - 1$ for a relatively small value of n, and those numbers do not have too many prime factors. This argument allows one to handle q larger than (roughly) $\sqrt{x}$. In more detail, let S denote the set of primes $p \le x$ for which C_q is satisfied for some $q > \sqrt{x}(\log x)$. Then $\mathrm{ord}_p(a) \le \sqrt{x}/(\log x)$, and thus $p \mid a^n - 1$ for some $n \le \sqrt{x}/(\log x)$. It follows that

$$\prod_{n \le \sqrt{x}/(\log x)} (a^n - 1) \equiv 0 \left(\mathrm{mod} \prod_{p \in S} p \right).$$

The left hand side is $a^{O(x/(\log x)^2)}$, from which we get $|S| = O(x/(\log x)^2) = o(\pi(x))$.

There is a small set of primes q near the value $\sqrt{x}$ that remains, namely the interval $q \in [\sqrt{x}/(\log x)^{B+2}, \sqrt{x}(\log x)]$. The idea here is to drop the power residue

condition in C_q and merely consider the congruence condition via

$$|\{p \le x : p \text{ satisfies } C_q\}| \le |\{p \le x : p \equiv 1 \pmod q\}|.$$

This loses a lot of information, but the bound above is sufficient as there are only few primes q left. Indeed, the right hand side may be bounded by the Brun–Titchmarsh inequality, giving the bound

$$|\{p \le x : p \equiv 1 \pmod q\}| \ll \frac{\pi(x)}{q}$$

for $q \le x^{1-\epsilon}$ for fixed $\epsilon > 0$, and we have

$$\sum_{\sqrt{x}/(\log x)^{B+2} \le q \le \sqrt{x}(\log x)} \frac{1}{q} = o(1)$$

by Mertens' theorem (or by the stronger prime number theorem and dyadic decomposition). This concludes the proof of (5.2.2) under GRH.

5.5 Schinzel–Wójcik problem

We then consider Problem 2.0.6. The problem was motivated by a work of Schinzel and Wójcik [42], where it was shown by elementary means that for any $a, b \in \mathbb{Q}^\times \setminus \{-1, 1\}$ there are infinitely many primes p with $\mathrm{ord}_p(a) = \mathrm{ord}_p(b)$. See also [51] and [37] for subsequent work.

We assume GRH. We first note that Hooley's argument adapts equally well to considering indices of multiple integers simultaneously. This observation was already implicitly present in Matthews' [34] work on simultaneous primitive roots, though it was not combined to the systematic framework above prior to our work.

We fix some integer h and consider the set of primes p such that $\mathrm{ord}_p(a_i) = (p-1)/h$. Instead of computing explicit formulas for the density of such p, which would be very laborious, it is better to think of reasons why there could be only finitely many such primes p. By the same procedure as in Artin's conjecture, the problem is reduced from considering infinitely many conditions C_q at once to merely finitely many of them, the conditions C_q now being that, for all i,

$$\begin{aligned}
&p \equiv 1 \pmod{q^{v_q(h)}}, \text{ and} \\
&a_i \text{ is a } q^{v_q(h)}\text{th power modulo } p, \text{ and} \\
&(p \not\equiv 1 \pmod{q^{v_q(h)+1}} \text{ or } a_i \text{ is not a } q^{v_q(h)+1}\text{th power modulo } p).
\end{aligned}$$

Again, these conditions are best viewed through field and Galois theory. Via the Artin symbol and the Chebotarev density theorem the problem above reduces to asking: is there, for any distinct primes $q_1, \dots, q_k$, necessarily some automorphism σ of

$$\mathbb{Q}(\zeta_{hq_1\cdots q_k}, a_1^{1/(hq_1\cdots q_k)}, \dots, a_n^{1/(hq_1\cdots q_k)})/\mathbb{Q}$$

that fixes $\mathbb{Q}(\zeta_h, a_1^{1/h}, \ldots, a_n^{1/h})$ but does not fix $\mathbb{Q}(\zeta_{hq_j}, a_i^{1/(hq_j)})$ for any i and j?

It turns out that primes q_i larger than 3 do not cause any issues. The idea is that roots of unity $\zeta_{q^v}, q \geq 5, v \geq 1$ do not lie in other extensions of form $\mathbb{Q}(\zeta_m, a_1^{1/m}, \ldots, a_n^{1/m})$ in a non-trivial way (that is, if m is not divisible by q^v), allowing one to construct σ so that it does not fix ζ_{hq_i} (but still fixing ζ_h). This corresponds to restricting to primes p such that $v_q(p-1) = v_q(h)$. In fact, by choosing h of form $3 \cdot 2^v$ for some v, one can similarly avoid issues at the prime 3, as ζ_9 does not lie non-trivially in root extensions.

So one only has to consider obstructions caused by the prime 2. Hence the problem more or less reduces to finding those tuples $(a_1, \ldots, a_n)$ for which there are infinitely many primes p such that

$$v_2(\mathrm{ord}_p(a_1)) = \ldots = v_2(\mathrm{ord}_p(a_n)).$$

This is where the obstruction of Theorem 5.0.1 comes in. First note that if for some integers $e_1, \ldots, e_n$ we have

$$a_1^{e_1} \cdots a_n^{e_n} = -1.$$

then all of $\mathrm{ord}_p(a_i)$ must be even: indeed, if $\mathrm{ord}_p(a_i) = O$ for all i, then

$$(-1)^O = (a_1^{e_1} \cdots a_n^{e_n})^O \equiv 1 \pmod{p}.$$

On the other hand, if for some integers f_i with an odd sum we have

$$a_1^{f_1} \cdots a_n^{f_n} = 1,$$

then O cannot be even, as otherwise $a_j^{O/2} \equiv -1 \pmod{p}$ for each j and thus

$$1 = 1^{O/2} \equiv (a_1^{f_1} \cdots a_n^{f_n})^{O/2} \equiv (-1)^{f_1 + \ldots + f_n} \equiv -1 \pmod{p}.$$

Hence if such tuples e_i and f_i exist, there are only finitely many desired primes p.

This turns out to be the only obstruction. The proof consists of tracking multiplicative relations between $a_1, \ldots, a_n$ (in particular, considering whether integers $e_1, \ldots, e_n$ as above exist) and considering basis elements $b_i, 1 \leq i \leq B$ for the group $\langle a_1, \ldots, a_n \rangle$ (or $\langle |a_1|, \ldots, |a_n| \rangle$). All relevant information on the orders $\mathrm{ord}_p(a_i)$ may then be written in terms of b_i via the Artin symbol and automorphisms of the field

$$\mathbb{Q}(\zeta_{2^k}, b_1^{1/2^k}, \ldots, b_B^{1/2^k}).$$

Here k is a large integer. As the elements b_i are multiplicatively independent, by the "almost maximality" of extensions as above (see [40] or Lemma 6.2.1) one may prescribe the images of $b_i^{1/2^k}$ under an automorphism more or less independently of each other and the image of ζ_{2^k}, while ensuring that a corresponding automorphism

in fact exists. One then has to decide on the images of $b_i^{1/2^k}$ and ζ_{2^k} so that the images of $a_i^{1/2^k}$ come out correct. This problem corresponds to satisfying a system of linear equations modulo 2, whose solvability is well understood.

Article III includes other applications of the methods as well, those following by broadly similar ideas and methods. These applications are somewhat *ad hoc*, calling for a more systematic approach, carried out in Article IV.

6 Unified treatment of Artin-type problems

We continue the discussion of Artin-type problems undertaken in Section 5. We start with introducing the general framework, after which we give some algebraic tools. We then discuss our ideas for treating Artin-type problems in general.

The following theorem captures a large portion of our results.

***Theorem* 6.0.1.** *Assume GRH. Let $W_1, \dots, W_n$ be finitely generated subgroups of $\mathbb{Q}^\times$. There is an explicit finite procedure for computing the image of the index map $\Psi : \mathbb{P} \to \mathbb{N}^n$,*

$$p \mapsto (\text{Ind}_p(W_1), \dots, \text{Ind}_p(W_n)).$$

Furthermore, if for any i we have

$$\text{rank } (W_1 \cdots W_n) > \text{rank } (W_1 \cdots W_{i-1} W_{i+1} \cdots W_n),$$

then there exists an integer H such that $(h_1, \dots, h_n)$ lies in the image of Ψ if and only if $((h_1, H), \dots, (h_n, H))$ does.

Our proof allows for other descriptions of the image of the index map as well, though they are more complicated.

6.1 General framework

There are several ways of generalizing Artin's conjecture.

First, instead of considering primitive roots ($\text{ord}_p(a) = p - 1$), consider near-primitive roots ($\text{ord}_p(a) = (p-1)/h$).

Second, consider the orders of multiple integers simultaneously as in Problem 2.0.6.

Third, instead of considering all primes, restrict to primes p in some "interesting" subset of integers. For example, one may restrict to primes in a given arithmetic progression. More generally, one could impose an Artin symbol condition on p, in particular allowing conditions of form "$p \equiv a \pmod m$" or "$P(x) \equiv 0 \pmod p$ is solvable" for given $P \in \mathbb{Z}[x]$. An Artin symbol condition is natural due to the algebraic number theoretic aspects of Artin's conjecture.

Fourth, instead of considering the reduction of a rational modulo p, one may consider reductions of a multiplicative subgroup W of $\mathbb{Q}^\times$, for example the order of the reduction of $W = \langle 2, 3 \rangle = \{2^n 3^m | n, m \in \mathbb{Z}\}$. It is reasonable to restrict to finitely generated subgroups W, that is, those subgroups for which there exist a finite set of generators $w_1, \dots, w_n \in W$ such that $W \subset \langle w_1, \dots, w_n \rangle$.

Finally, one may consider the problems over an arbitrary number field K in place of $\mathbb{Q}$, replacing the primes p of $\mathbb{Q}$ with the prime ideals $\mathfrak{p}$ of K (or, more precisely, prime ideals of the ring of integers of K). For expository reasons, here we consider problems simply over $\mathbb{Q}$ – generalizing to arbitrary K requires no major changes.

These generalizations bring us to the index map problem (Problem 2.0.7). One notes that many previous problems can be seen as specific instances of the general one: Artin's conjecture asks when the image of $p \mapsto \text{Ind}_p(a)$ contains 1 infinitely often, simultaneous primitive roots correspond to the preimage of $(1, \dots, 1)$ under $p \mapsto (\text{Ind}_p(a_1), \dots, \text{Ind}_p(a_n))$, the Schinzel–Wójcik problem concerns the preimage of $\{(h, \dots, h) | h \in \mathbb{N}\}$ and so on. We note that Lenstra [29] has considered a setup almost as general, namely the case $n = 1$ of Problem 2.0.7.

We cannot give an explicit description of the image of the index map of Problem 2.0.7 in the general case, as such a description would be too complex. Rather, we give a computational procedure that may be used to determine the index map, and via inspection of the procedure obtain non-trivial descriptions of the image.

6.2 Algebraic tools

We first repeat the general principle that questions on sets of primes defined via solvability of polynomial congruences are best viewed through the lens of field theory. A powerful tool ere is the *Artin symbol*, which unfortunately we cannot properly explain here due to the technical nature. However, at a very broad level, the Artin symbol connects the primes p for which a given polynomial congruence $P(x) \equiv 0 \pmod{p}$ is solvable to an object of a number field K containing the roots of $P(x)$. This establishes a connection between *local* and *global* structures.

To get some taste of the connection, let us give a simple example. Consider the congruence $x^2 + 1 \equiv 0 \pmod{p}$ and the corresponding number field $K = \mathbb{Q}(i)$. The odd primes p for which the congruence is solvable (namely $p \equiv 1 \pmod{4}$) are associated to the identity map $a + bi \to a + bi$ of K, whereas the other odd primes are associated to the conjugation map $a + bi \to a - bi$. (The prime $p = 2$ is a special case we ignore.)

In general, primes get associated to automorphisms of the corresponding number field depending on what kind of polynomial equations are solvable locally. (To be more precise and general, one should talk about homomorphisms from the ring of integers of K to finite fields of size $p^k, k \geq 1$ – these homomorphisms are vital for connecting global and local structures, and the Artin symbol is defined to capture

information regarding these homomorphisms.)

Via these tools one may connect knowledge on the complex roots of polynomials to information on the local polynomial equations. Furthermore, the Chebotarev density theorem tells us how often the primes associate to given automorphisms as one goes through all of the primes.

As particularly important special cases, power congruences $x^n \equiv a \pmod p$ and congruence conditions $p \equiv r \pmod m$ are linked to the fields $\mathbb{Q}(\zeta_n, a^{1/n})$ and $\mathbb{Q}(\zeta_m)$, respectively. We have already described how non-trivial interactions or failure of maximality of such extensions leads to surprising phenomena and obstructions in Artin's conjecture and related problems.

Fortunately for us, there turn out to be, in a sense, only finitely many such obstructions and issues in any given situation. More precisely, root extensions are "almost maximal" in degree [40].

***Lemma* 6.2.1** (Almost maximality of root extensions)**.** *Let $a_1, \dots, a_r \in \mathbb{Q}^\times$ be multiplicatively independent. There is some constant $c > 0$ (depending on a_i only) such that for any $m \in \mathbb{N}$ we have*

$$[\mathbb{Q}(\zeta_m, a_1^{1/m}, \dots, a_r^{1/m}) : \mathbb{Q}] \geq c\phi(m)m^r.$$

Following the same theme, there is only a finite amount of non-trivial interaction between the various root extensions (see Article IV, Proposition 3.1).

***Lemma* 6.2.2** (Finite interaction of root extensions)**.** *Let $a_1, \dots, a_r \in \mathbb{Q}^\times$ be multiplicatively independent. There is a number field F (depending on a_i only) such that for any coprime m_1 and m_2 we have*

$$\mathbb{Q}(\zeta_{m_1}, a_1^{1/m_1}, \dots, a_r^{1/m_1}) \cap \mathbb{Q}(\zeta_{m_2}, a_1^{1/m_2}, \dots, a_r^{1/m_2}) \subset F.$$

Especially important are the consequences for the set of automorphisms of such root extensions (the *Galois groups* of the extensions). As any automorphism maps elements to their conjugates, the root of unity ζ_m is mapped to ζ_m^x for some x coprime to m and $a_i^{1/m}$ is mapped to $\zeta_m^{x_i} a_i^{1/m}$ for some integer x_i. Also, the values of x and x_i determine the automorphism uniquely. However, as the extension is not necessarily maximal, not all values of $(x, x_1, \dots, x_r)$ correspond to an automorphism. Nevertheless, in the same spirit as the results above, whether or not there is a corresponding automorphism depends only on the values of x and x_i modulo M for some fixed M.

Finally, regarding the finitely generated multiplicative groups we mention the following.

***Lemma* 6.2.3** (Bases for subgroups)**.** *Let W be a finitely generated subgroup of $\mathbb{Q}^\times$. Then there is an integer r and $w_1, \dots, w_n \in W$ such that any $w \in W$ may be expressed uniquely as*

$$w = (-1)^{e_0} w_1^{e_1} \cdots w_n^{e_n}, e_i \in \mathbb{Z}, e_0 \in \{0, 1\}.$$

A corresponding result is true for any number field K in place of $\mathbb{Q}$, with -1 replaced with ζ_k for the largest k with $\zeta_k \in K$. The result follows from the classification of finitely generated abelian groups.

6.3 Proof methods

We then consider the general setup of Problem 2.0.7, with the aim of describing the image of the index map. For simplicity, we shall work over $\mathbb{Q}$ and will not consider an additional Artin symbol condition on p, as these lead into minor technical differences only.

We fix finitely generated subgroups $W_1, \dots, W_n$ of $\mathbb{Q}^\times$ and consider the values of the index map

$$\Psi(p) := (\text{Ind}_p(W_1), \dots, \text{Ind}_p(W_n)).$$

We fix some tuple $\mathbf{h} = (h_1, \dots, h_n)$, and consider whether the set of primes p with $\Psi(p) = \mathbf{h}$ is infinite or not. We provide an explicit procedure for determining whether this is the case.

As with Artin's primitive root conjecture, one can use certain analytic methods (conditional on GRH) to reduce this problem to determining whether for any finite number of primes $q_1, \dots, q_n$ certain conditions may be met. More precisely, for $Q = q_1 \cdots q_n$ we aim to determine whether there exists an automorphism of

$$K_{Q,\mathbf{h}} := \mathbb{Q}(\zeta_{Qh}, W_1^{1/h_1 q_1}, \dots, W_n^{1/h_n q_n})$$

fixing all of the fields $\mathbb{Q}(\zeta_{h_i}, W_i^{1/h_i})$ but none of $\mathbb{Q}(\zeta_{qh_i}, W_i^{1/qh_i})$ for $q \mid Q$. Here $h = \text{lcm}(h_1, \dots, h_n)$, and $K(W^{1/h})$ means the smallest extension of K containing ζ_h and $w^{1/h}$ for any $w \in W$.

We first reduce to the case where Q has no "large" prime factors. More precisely, if $q > 3$ and q does not divide h, one has $\zeta_q \notin K_{Q,\mathbf{h}}$ for any $q \nmid Q$, and hence an admissible automorphism of $K_{Q,\mathbf{h}}$ may be extended to $K_{Qq,\mathbf{h}}$ so that it does not fix ζ_q.

Assume then that $Q \mid 6h$. The next step is to reduce the problem to considering just the case where Q is a prime. This would be easy if $K_{q,\mathbf{h}} \cap K_{q',\mathbf{h}} = K_{1,\mathbf{h}}$ for any distinct primes $q, q' \mid Q$, but this is unfortunately not necessarily the case. However, by Lemma 6.2.2 such intersections cannot be much larger than $K_{1,\mathbf{h}}$. One can hence perform a finite casework on the behavior of the automorphism in such intersections, after which the extensions $K_{q,\mathbf{h}}/K_{1,\mathbf{h}}$ are practically independent of each other.

We thus consider whether there exists an automorphism of $K_{q,\mathbf{h}}$ fixing $K_{1,\mathbf{h}}$, not fixing any of $\mathbb{Q}(\zeta_{qh_i}, W_i^{1/qh_i})$ and satisfying a certain additional condition arising from the previous step. The idea is that the extension $K_{q,\mathbf{h}}$ is "almost maximal" (see Lemma 6.2.1), so that the Galois group $\text{Gal}(K_{q,\mathbf{h}}/K_{1,\mathbf{h}})$ is easy to describe in images of generators of W_i (recall Lemma 6.2.3). Complications arise from the fact

that $W_1, \ldots, W_n$ need not be multiplicatively independent of each other, or that basis elements of W_i may be perfect qth powers or their products may non-trivially yield qth powers.

We proceed by carefully keeping track of the "parts" in groups W_i that are independent of the other groups, categorizing the groups depending on the sizes of valuations $v_q(h_i)$ and handling separately groups whose valuations differ significantly in size. We are able to reduce the problem to a system of linear congruences and incongruences modulo powers of q, from which one may compute whether a solution exists in an effective manner.

It is essential that the computation in the last part takes only a bounded amount of time, so that the number of steps in the whole process for determining whether $\mathbf{h}$ lies in the image of Ψ is bounded by a linear function in the number of distinct prime factors of $\operatorname{lcm}(h_1, \ldots, h_n)$ (assuming that operations with arbitrarily large integers take negligible time).

Furthermore, by inspecting the proof one obtains a description of the image of Ψ. Namely, one obtains that if a prime q and $I \subset \{1, \ldots, n\}$ are such that $\min_{i \in I, j \in \{1,\ldots,n\} \setminus I} |v_q(h_i) - v_q(h_j)|$ is large enough (in terms of parameters arising from $K, W_1, \ldots, W_n$), then $(h_1, \ldots, h_n)$ is in the image if and only if $(h'_1, \ldots, h'_n)$ is, where $h'_i = qh_i$ for $i \in I$ and $h'_j = h_j$ for $j \notin I$. In other words, we may increase the q-adic valuation of some elements, assuming that those q-adic valuations are sufficiently "isolated" from the other valuations.

We further note that one may give simpler descriptions for the image of Ψ in the case the groups $W_1, \ldots, W_n$ are *separated*, meaning that the rank of $W_1 \cdots W_n$ is strictly larger than the rank of $W_1 \cdots W_{i-1} W_{i+1} \cdots W_n$ for any i. This means that for each W_i there is an element $w_i \in W_i$ which is independent of the group $W_1 \cdots W_{i-1} W_{i+1} \cdots W_n$, allowing one to control $\operatorname{Ind}_p(W_i)$ more freely. We are able to show that in this case there is some $H \in \mathbb{N}$ such that $(h_1, \ldots, h_n)$ lies in the image of Ψ if and only if $((h_1, H), \ldots, (h_n, H))$ does.

We again guide the reader to the original article for details of the proofs and other results not presented here.

List of References

[1] T. M. Apostol. *Introduction to analytic number theory*. Springer Science & Business Media, 1998.

[2] R. C. Baker, G. Harman, and J. Pintz. The difference between consecutive primes, II. *Proc. Lond. Math. Soc.*, 83(3):532–562, 2001.

[3] G. Cooke and P. J. Weinberger. On the construction of division chains in algebraic number rings, with applications to SL_2. *Comm. Algebra*, 3(6):481–524, 1975.

[4] H. Cramér. On the order of magnitude of the difference between consecutive prime numbers. *Acta Arith.*, 2:23–46, 1936.

[5] J.-M. Deshouillers and H. Iwaniec. An additive divisor problem. *J. London Math. Soc. (2)*, 26(1):1–14, 1982.

[6] P. Erdös and M. Ram Murty. On the order of $a \pmod p$. In *CRM Proceedings and Lecture Notes*, volume 19, pages 87–97, 1999.

[7] S. W. Graham and G. Kolesnik. *van der Corput's method of exponential sums*, volume 126 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1991.

[8] A. Granville. Harald Cramér and the distribution of prime numbers. *Scand. Actuar. J.*, 1995(1):12–28, 1995.

[9] A. Granville. Pretentiousness in analytic number theory. *J. Théor. Nombers. Bordeaux*, 21(1):159–173, 2009.

[10] A. Granville, A. Harper, and K. Soundararajan. A more intuitive proof of a sharp version of Halász's theorem. *Proc. Amer. Math. Soc.*, 146(10):4099–4104, 2018.

[11] A. Granville and K. Soundararajan. Pretentious multiplicative functions and an inequality for the zeta-function. In *CRM Proceedings and Lecture Notes*, volume 46, 2008.

[12] G. Halász. Über die Mittelwerte multiplikativer zahlentheoretischer Funktionen. *Acta Math. Acad. Sci. Hungar.*, 19(3-4):365–403, 1968.

[13] G. Halász. On the distribution of additive and the mean values of multiplicative arithmetic functions. *Studia Sci. Math. Hungar.*, 6:211–233, 1971.

[14] G. Harman. *Prime-detecting sieves*, volume 33 of *London Mathematical Society Monographs Series*. Princeton University Press, Princeton, NJ, 2007.

[15] G. Harman and P. Lewis. Gaussian primes in narrow sectors. *Mathematika*, 48(1-2):119–135 (2003), 2001.

[16] D. R. Heath-Brown. The differences between consecutive primes. *J. Lond. Math. Soc.*, 2(1):7–13, 1978.

[17] D. R. Heath-Brown. The differences between consecutive primes, III. *J. Lond. Math. Soc.*, 2(2):177–178, 1979.

[18] D. R. Heath-Brown. Gaps between primes, and the pair correlation of zeros of the zeta-function. *Acta Arith.*, 41:85–99, 1982.

[19] D. R. Heath-Brown. Artin's conjecture for primitive roots. *Q. J. Math.*, 37(1):27–38, 1986.

[20] D. R. Heath-Brown. The number of primes in a short interval. *J. Reine Angew. Math.*, 389:22–63, 1988.

[21] D. R. Heath-Brown. The differences between consecutive smooth numbers. *Acta Arith.*, 184:267–285, 2018.

[22] D. R. Heath-Brown. The differences between consecutive primes, V. *Int. Math. Res. Not. IMRN*, 2021(22):17514–17562, 2020.
[23] C. Hooley. On Artin's conjecture. *J. Reine Angew. Math.*, 225:209–220, 1967.
[24] B. Huang, J. Liu, and Z. Rudnick. Gaussian primes in almost all narrow sectors. *Acta Arith.*, 193(2):183–192, 2020.
[25] H. Iwaniec and E. Kowalski. *Analytic number theory*, volume 53 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2004.
[26] O. Järviniemi. Polynomial and exponential equations modulo primes. Master's thesis, University of Helsinki, 2021.
[27] C. Jia. Almost all short intervals containing prime numbers. *Acta Arith.*, 76(1):21–84, 1996.
[28] S. Lang. On the zeta function of number fields. *Invent. Math.*, 12(4):337–345, 1971.
[29] H. W. Lenstra, Jr. On Artin's conjecture and Euclid's algorithm in global fields. *Invent. Math.*, 42:201–224, 1977.
[30] P. A. Lewis. Finding information about Gaussian primes using analytic number theory sieve methods. Ph.D. thesis, Cardiff University, 2002.
[31] K. Matomäki. Large differences between consecutive primes. *Q. J. Math.*, 58(4):489–518, 2007.
[32] K. Matomäki and M. Radziwiłł. Multiplicative functions in short intervals. *Ann. of Math.*, pages 1015–1056, 2016.
[33] K. Matomäki and J. Teräväinen. Almost primes in almost all short intervals II. *To appear in Trans. Amer. Math. Soc.*, 2023.
[34] K. Matthews. A generalisation of Artin's conjecture for primitive roots. *Acta Arith.*, 29(2):113–146, 1976.
[35] P. Moree. Artin's primitive root conjecture -a survey -. *Integers*, 12, 01 2005.
[36] P. Moree and P. Stevenhagen. A two-variable Artin conjecture. *J. Number Theory*, 85(2):291–304, 2000.
[37] F. Pappalardi and A. Susa. On a problem of Schinzel and Wójcik involving equalities between multiplicative orders. *Math. Proc. Cambridge Philos. Soc.*, 146:303 – 319, 03 2009.
[38] A. S. Peck. *On the differences between consecutive primes.* PhD thesis, University of Oxford, 1996.
[39] A. S. Peck. Differences between consecutive primes. *Proc. Lond. Math. Soc.*, 76(1):33–69, 1998.
[40] A. Perucca and P. Sgobba. Kummer theory for number fields and the reductions of algebraic numbers. *Int. J. Number Theory*, 15(08):1617–1633, 2019.
[41] S. J. Ricci. *Local distribution of primes*. ProQuest LLC, Ann Arbor, MI, 1976. Thesis (Ph.D.)–University of Michigan.
[42] A. Schinzel and J. Wójcik. On a problem in elementary number theory. *Math. Proc. Cambridge Philos. Soc.*, 112(2):225–232, 1992.
[43] K. Soundararajan. The Liouville function in short intervals [after Matomäki and Radziwiłł]. *arXiv preprint arXiv:1606.08021*, 2016.
[44] J. Stadlmann. On the mean square gap between primes. *arXiv preprint arXiv:2212.10867*, 2022.
[45] P. Stevenhagen and H. W. Lenstra. Chebotarëv and his density theorem. *Math. Intelligencer*, 18:26–37, 1996.
[46] J. Teräväinen. Almost primes in almost all short intervals. *Math. Proc. Cambridge Philos. Soc.*, 161(2):247–281, 2016.
[47] E. C. Titchmarsh. *The theory of the Riemann zeta-function*. Oxford university press, 1986.
[48] H. von Koch. Sur la distribution des nombres premiers. *Acta Math.*, 24(1):159–182, 1901.
[49] S. Wagstaff. Pseudoprimes and a generalization of Artin's conjecture. *Acta Arith.*, 41(2):141–150, 1982.
[50] D. Wolke. Große Differenzen zwischen aufeinanderfolgenden Primzahlen. *Math. Ann.*, 218(3):269–271, 1975.
[51] J. Wójcik. On a problem in algebraic number theory. *Math. Proc. Cambridge Philos. Soc.*, 119(2):191–200, 1996.
[52] G. Yu. The differences between consecutive primes. *Bull. Lond. Math. Soc.*, 28(3):242–248, 1996.

[53] A. Zaccagnini. Primes in almost all short intervals. *Acta Artih.*, 84(3):225–244, 1998.

TURUN
YLIOPISTO
UNIVERSITY
OF TURKU

ISBN 978-951-29-9304-8 (PRINT)
ISBN 978-951-29-9305-5 (PDF)
ISSN 0082-7002 (Print)
ISSN 2343-3175 (Online)

Painosalama Oy, Turku, Finland 2023