COUNTING PRIMES

JAMES MAYNARD

ABSTRACT

We survey techniques used to detect prime numbers in sets, highlighting the strengths and limitations of current techniques.

MATHEMATICS SUBJECT CLASSIFICATION 2020

Primary 11N05; Secondary 11N35, 11M06, 11N13

KEYWORDS

Prime numbers, sieve methods, Type I/II sums

INTERNATIONAL CONGRESS
OF MATHEMATICIANS
2022 JULY 6—14

Proc. Int. Cong. Math. 2022, Vol. 1, pp. 240–268
DOI 10.4171/ICM2022/206

Published by EMS Press

1. INTRODUCTION

Many of the most notorious open problems about prime numbers can be phrased as variations of the following question.

Question. Given a set of integers $\mathcal{A}$, how many primes are in $\mathcal{A}$?

Depending on the context, 'how many' could be asking whether there exists at least one prime in $\mathcal{A}$, whether there are infinitely many primes in $\mathcal{A}$, or asking for a quantitative estimate for the number of primes up to some threshold.

For example, we have the following special cases:

- $\mathcal{A} = \mathbb{Z}$. That there are infinitely many primes in $\mathcal{A}$ follows from Euclid's proof of the infinitude of primes. An asymptotic formula for the primes in $\mathcal{A}$ less than x is given by the Prime Number Theorem, and asking for the smallest possible error term in such an asymptotic estimate is essentially a reformulation of the Riemann Hypothesis.

- $\mathcal{A} = \{p + 2 : p \text{ prime}\}$. Asking for infinitely many primes in $\mathcal{A}$ is the famous Twin Prime Conjecture, and an asymptotic formula for the number of primes in $\mathcal{A}$ is a conjecture of Hardy and Littlewood.

- $\mathcal{A} = \{2N - p : p \text{ prime}\}$, for some fixed integer $N \geq 2$. In this case $\mathcal{A}$ contains only a finite number of positive elements (and so a finite number of primes), but asking that it contains at least one prime for every $N \geq 2$ is Goldbach's conjecture.

The final two examples are two of Landau's influential four problems on primes listed in his 1912 ICM address; all four remain unsolved.

In general, we will focus on situations where we expect (from heuristics, numerical evidence, or other guesswork) that there should be primes in $\mathcal{A}$, and the task is to try to prove this is indeed the case.

We know of no way to *construct* prime numbers theoretically, and therefore we typically need to use an indirect method to prove the existence of primes in a given set $\mathcal{A}$. If we are unable to numerically test elements, then often the only way we know how to prove the existence of a single prime in a set $\mathcal{A}$ is to perform the a priori harder task of approximately counting the number of primes in $\mathcal{A}$ and showing there are many primes in $\mathcal{A}$ of a given size. For example, Vinogradov's three primes theorem states that every sufficiently large odd number can be written as the sum of three primes (this is now actually known for *all* $N \geq 7$ thanks to work of Helfgott [42]), but the only way we know how to prove this actually shows that there are 'many' ways to write a large odd integer N as the sum of three primes.

The ultimate goal in this area is to develop a flexible toolkit which can reduce the question of counting primes in sets $\mathcal{A}$ of interest to easier (but more technical) questions about the arithmetic structure of the set in question, and then to have a set of techniques which can investigate these questions.

2. MULTIPLICATIVE NUMBER THEORY

Multiplicative number theory rests on utilizing the following crucial property of the primes, which is essentially the Fundamental Theorem of Arithmetic.

Property. Prime numbers generate the positive integers via multiplication.

This property allows us to define suitable multiplicative generating functions (L-functions) which encode properties of the primes via the integers they generate. A reformulation of the Fundamental Theorem of Arithmetic is the identity (for $\mathrm{Re}(s) > 1$)

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p} \left(1 - \frac{1}{p^s}\right)^{-1}.$$

Since we analytically understand the integers under addition quite well, we can obtain a good understanding (analytic continuation, controlled growth) of $\zeta(s)$ via the Dirichlet series representation on the left-hand side. This understanding can then be translated into understanding about the primes. The infinitude of the primes follows from the fact that $\zeta(s)$ has a pole at $s = 1$, the Prime Number Theorem follows from (and is essentially equivalent to) the fact that $\zeta(s)$ has no zeros on the line $\mathrm{Re}(s) = 1$, and precise estimates for the count of primes are essentially equivalent to zero-free regions for $\zeta(s)$ within the critical strip $0 < \mathrm{Re}(s) < 1$. In all these cases the partial information we are interested in about primes becomes much easier to establish via translating it to a question about partial understanding of $\zeta(s)$.

Moreover, the techniques of multiplicative number theory extend well beyond just studying primes via $\zeta(s)$, but to a whole zoo of different L-functions which encode different algebraic information about primes. Prime ideals generate all ideals of the ring of integers of a number field, and so prime ideals (and hence the splitting of rational primes) can be studied via the same techniques via Dedekind L-functions $\zeta_K(s)$ (the analogue of $\zeta(s)$ for a number field K). Moreover, one can twist the $\zeta(s)$ by a Dirichlet character or the Archimedean character n^{it}, or one can twist $\zeta_K(s)$ by a Hecke character (or more generally twist an L-function by a suitable automorphic representation), to obtain further L-functions, which can study primes in arithmetic progressions, short intervals, the locations of prime ideals in lattices or similar questions.

Essentially the *only* method we have which is capable of 'producing' primes is using multiplicative number theory. Even though there are now a few ostensibly different proofs of the Prime Number Theorem, all known proofs rely fundamentally on the Fundamental Theorem of Arithmetic, and require multiplicative structure. Virtually all other results counting primes can be thought of as extensive elaborate manoeuvres which allow one to reduce to the situation of using multiplicative number theory to count primes.

2.1. Primes and zeros

The techniques of multiplicative number theory crucially allow one to understand multiplicative questions on the distribution of primes via the zeros of the corresponding L-functions. The duality between primes and zeros of $\zeta(s)$ is best seen through Riemann's famous *Explicit Formula* for $\zeta(s)$: for $x, T \geq 2$,

$$\sum_{n<x} \Lambda(n) = x - \sum_{|\rho|<T} \frac{x^\rho}{\rho} - \log\big(2\pi\sqrt{1-x^{-2}}\big) + O\bigg(\frac{x(\log x)^3}{T}\bigg), \tag{2.1}$$

where $\Lambda(n)$ is the von Mangold function and the sum is over all nontrivial zeros ρ of $\zeta(s)$ (counted with multiplicity, although all zeros are believed to be simple). For every L-function (satisfying the expected meromorphicity and growth conditions), we get a corresponding explicit formula with one side representing primes and the other zeros of the L-function.

The explicit formula points to unexpected deep *structure* within the sequence of primes; if the Riemann Hypothesis ($\mathrm{Re}(\rho) = 1/2$ for all nontrivial ρ) holds, then treating all terms apart from x trivially, we would obtain a *smaller* size error term than we would expect based on simple random model predictions (we expect that the presence of zeros alters effects such as the law of the iterated logarithm, for example). Indeed, the zeros of $\zeta(s)$ constrain the error term in the count of primes to fluctuate relatively less than we expect for other arithmetic sequences (such as twin primes) where we expect 'random-like' behavior. Another example where this structure plays a role is the fact that the error term in the Prime Number Theorem can be self-improving; if we can show that

$$\left|\pi(x) - \int_2^x \frac{dt}{\log t}\right| \ll x^{1/2+o(1)},$$

then we know that the Riemann Hypothesis holds and the error term $x^{1/2+o(1)}$ can be upgraded to the more precise $O(x^{1/2}\log x)$. It would be interesting to see if the structure implied by zeros can be exploited meaningfully in other ways.

Similarly, since the error term in (2.1) disappears as $T \to \infty$, we see that knowing *all* zeros encodes *all* information about primes, and vice versa. This observation is useless for most practical purposes, but it means that zeros of $\zeta(s)$ must also encode the distribution of primes in arithmetic progressions, and therefore encode information about zeros of Dirichlet L-functions too. This is partial justification for the idea that L-functions should be studied in families rather than individually. A spectacular example of this is Goldfeld and Gross–Zagier's [29, 30, 34] joint resolution of the Gauss class number one problem by showing that an L-function attached to a suitable Elliptic curve had a triple zero at the central point, and this triple zero had a suitably strong influence on zeros of Dirichlet L-functions to prevent there being any particularly bad Siegel zeros.

2.2. Zero density estimates

Although the Riemann Hypothesis is the most important question for any given L-function, often it would suffice for applications to primes to show a much weaker statement that 'most' zeros lie 'close' to the line $\mathrm{Re}(s) = 1/2$, rather than requiring that all zeros lie on this line. For example, under the Riemann Hypothesis we can show an asymptotic formula for primes in $[x, x + x^{1/2}(\log x)^2]$. If we let $N(\sigma, T)$ denote the number of zeros $\rho = \beta + i\gamma$ with $|\gamma| \leq T$ and $\beta \geq \sigma$ then a bound $N(\sigma, T) \ll T^{2-2\sigma+o(1)}$ (known as the 'Density Hypothesis') would allow us to deduce an asymptotic formula for primes in

$[x, x + x^{1/2+o(1)}]$, which is almost as short as what we obtain under the Riemann Hypothesis. Unfortunately, the Density Hypothesis is open in general, but a classical result of Huxley [44] shows $N(\sigma, T) \ll T^{12(1-\sigma)/5+o(1)}$, which implies an asymptotic formula for the number of primes in $[x, x + x^{7/12+o(1)}]$, and is essentially the best known result (Heath-Brown [36] used sieve methods to remove the $o(1)$.)

In many counting problems for the primes which are directly related to zeros, the limitation in our results is due to a limitation in our understanding of zeros near the 3/4-line (such as the example above of primes in short intervals), or near the 1-line (such as issues with Siegel zeros or the least quadratic nonresidue). For example, if we knew that there were no zeros ρ with $0.74 \leq \mathrm{Re}(\rho) \leq 0.76$ (or if there were 'few' such zeros), then we would improve on our understanding of primes in short intervals. The typical way to bound such zeros is to detect them via large values of a Dirichlet polynomial (see [47, CHAPTER 10]). The key limitation of our zero density estimates for the past 50 years reduces to the following question.

Question 1. Can we show

$$\mathrm{meas}\left\{t \in [T, 2T] : \left|\sum_{n=T^{2/5}}^{2T^{2/5}} n^{it}\right| > T^{3/10}\right\} \ll T^{3/5-\delta}$$

for some fixed positive constant δ?

The bound $T^{3/5+o(1)}$ follows quickly from straightforward bounds for the 4th or 6th mean value of the Dirichlet polynomial. Improving on the 6th moment bound is related to bounding the 6th moment of $\zeta(1/2 + it)$, but it is not unreasonable to hope that this question might be easier to study.

Even if we cannot improve our current zero-density bounds on the *number* of zeros, an alternative approach might be to see what this might imply for the *distribution* of zeros of $\zeta(s)$. (Ultimately one might hope to obtain a putative classification which either contradicts other known properties or demonstrates that there are still primes in short intervals with this distribution of zeros.)

Question 2. Imagine that $|\pi(x + x^{7/12-\epsilon}) - \pi(x) - x^{7/12-\epsilon}/\log x| \gg x^{7/12-\epsilon}/\log x$ for some large x. What does this imply about the distribution of the zeros of $\zeta(s)$?

We know that there must be roughly $T^{3/5}$ zeros of height T with real part very close to $3/4$ for $T \approx x^{5/12}$, and, moreover, it must be the case that these zeros $\rho = \beta + i\gamma$ have the fact that the fractional part of $2\pi\gamma \log x$ is quite strongly biased modulo 1. Moreover, we speculate that there should be much more prescriptive constraints on the *vertical* distribution such zeros – roughly that they occur in small clusters whose imaginary parts are roughly in an arithmetic progression. Obtaining a precise classification of this sort seems difficult (it appears related to the inverse Littlewood problem in additive combinatorics/harmonic analysis), but a suitably strong classification would open up a new manner to potentially rule out conspiracies preventing primes in short intervals. A proof-of-concept in this direction is recent work with Pratt [66].

Theorem 3 (Conditional improvement to zero density estimates). *Assume that the zeros of $\zeta(s)$ lie on finitely many vertical lines. Then*

$$\#\{p \in [x, x + x^{1/2+\epsilon}]\} = (1 + o_\epsilon(1))\frac{x^{1/2+\epsilon}}{\log x}.$$

The point here is that the hypothesis still allows for the possibility of vertical arithmetic progressions of zeros, and so one of the potential limitations is actually less of an issue. We can obtain improvements on the classical exponent 7/12 to give results almost as strong as what the Riemann Hypothesis would imply by studying the vertical patterns of zeros of $\zeta(s)$, albeit under rather strong assumptions.

In a very different direction, following work of Matomäki–Radziwiłł [54], if one is interested in the Möbius function (and is happy with weaker quantitative bounds), then we can restrict attention to Dirichlet polynomials which factor in many ways (expanding on earlier ideas of [8,10,49]). This allows one to overcome the issues raised here for primes, and obtain stronger results about the Möbius function in short intervals [56] as well as almost-all short intervals [54].

2.3. Limits to multiplicative techniques

In general the multiplicative theory for counting primes points to a rich structure encoded by the zeros and a powerful set of techniques. Unfortunately, there are some issues with this from a practical point of view:

(1) Multiplicative techniques rely on the presence of multiplicative structure in the problem. In situations which are less structured (particularly when there is addition polluting multiplicative objects like in the Twin Prime Conjecture), we do not know how to make use of multiplicative techniques. Even when they can be of use, it require a lot of work to massage problems into a suitable form that the powerful multiplicative techniques can apply to.

(2) In the absence of the conjectured strong control over zeros, our estimates are often limited in their range of applicability, particularly with uniformity of estimates with respect to underlying parameters such as conductor or degree of number field.

(3) The multiplicative methods tend to either give strong asymptotic formulae or fail to give any nontrivial bound whatsoever. The strength of the analytic approach means that it is not well-suited to answering ‘soft’ questions with a wide degree of flexibility.

As an example of the final two points, Hooley’s [43] proof of the Artin primitive root conjecture under the Generalized Riemann Hypothesis for suitable Dedekind L-functions relied crucially on the upper bound

$$\sum_{q\sim Q} \pi^*(x;q) \ll \frac{x}{Q\log x} + Qx^{1/2}(\log x)^{O(1)},$$

where $\pi^*(x;q)$ counts primes $p < x$ with $p \equiv 1 \pmod{q}$ and for which 2 is a qth power $\pmod{p}$. (In fact, an upper bound of the form $o_{Q\to\infty}(x/(\log x)^2)$ for $Q < x^{1/2}(\log x)^{-A}$ would have sufficed.) The only way we know how to prove an upper bound of this type is by proving an asymptotic formula of the form $\pi^*(x;q) = \pi(x)/(q\varphi(q)) + O(x^{1/2}\log x)$ via GRH, which is a much stronger statement. Unconditional techniques based on multiplicative number theory can capture the condition of being a qth power, but only with error terms that degrade quickly with q. (By contrast, other techniques such as sieve methods can be very flexible at producing upper bounds, but appear poorly suited to capturing the more algebraic qth power condition.)

Question 4. Can one produce a nontrivial upper bound for $\sum_{q\sim x^{1/2-\epsilon}} \pi^*(x;q)$ unconditionally?

3. SIEVE METHODS

Sieve methods take a different, combinatorial approach to studying primes, based on the following simple property:

Property. Primes are integers n which have no divisors smaller than $\sqrt{n}$ other than 1.

Thus primes are examples of numbers with no small divisors, and more generally one can look at integers n with no divisors (other than 1) less than some quantity z. This formulation naturally suggests that one can count such numbers in a set $\mathcal{A}$ via inclusion–exclusion:

$$\sum_{\substack{n\in\mathcal{A}\\ p|n\Rightarrow p>z}} 1 = \sum_{\substack{d\\ p|d\Rightarrow p\le z}} \mu(d) \sum_{\substack{n\in\mathcal{A}\\ d|n}} 1.$$

Let us restrict attention from now on to sets $\mathcal{A} \subseteq [x, 2x]$ for some large value x, so that all elements have roughly the same size.

Unfortunately, even if one had very good estimates for the size of the set $\mathcal{A}_d$ of multiples of d in $\mathcal{A} \subset [x, 2x]$, there would be $2^{\pi(z)}$ different integers d in the sum and so any error terms would accumulate and dominate the hope of a main term unless z was very small (such as if $z \le \log x$). The first key insight in of sieve methods is that one can use positivity to truncate the inclusion–exclusion process and avoid the presence of d's which are too large, at the cost of a small amount of precision. The basic arithmetic information required to make this work is then a moderate understanding of inner sums above, namely the size of the sets $\mathcal{A}_d = \{n \in \mathcal{A} : d|n\}$.

Let $g(d)$ be a multiplicative function which we think of as an approximation to the density of elements of $\mathcal{A}$ which are a multiple of d. We assume that $g(p) < 1 - \epsilon$ (so that there are no prime factors which are too common) and that $g(p) \approx \kappa/p$ for some fixed constant $\kappa > 0$ on average by assuming for $2 \le w$,

$$\sum_{p\le w} g(p)\log p = \kappa \log w + O(1). \tag{3.1}$$

The key arithmetic input for sieve methods is then an estimate for every $A > 0$,

$$\sum_{d<x^\gamma} \left|\#\mathcal{A}_d - g(d)\#\mathcal{A}\right| \ll_A \frac{\#\mathcal{A}}{(\log x)^A} \tag{3.2}$$

for some given fixed $\gamma > 0$. The larger we are able to take γ, the better we are able to understand $\mathcal{A}$ in arithmetic progressions and the more powerful the conclusions of our sieve methods will be. In most situations of interest we expect (3.2) to hold for a suitable function g and reasonably large constant $\gamma \in (0,1)$, so (3.2) should be thought of as a reasonably mild constraint when γ is small.

The basic point of sieve methods is that for any set which does satisfy an estimate like (3.2) we can make the inclusion-exclusion argument much more accurate. This is known as the 'fundamental lemma' (see, for example, [28, COROLLARY 6.10]).

Lemma 5 (Fundamental Lemma of Sieve Methods). *Let g be a multiplicative function as above. Then we have for any $\eta, \gamma > 0$,*

$$\sum_{\substack{n\in\mathcal{A}\\ p|n\Rightarrow p>x^\eta}} 1 = \left(1 + O_\kappa\left(e^{-\gamma/\eta}\right)\right) \prod_{p\le x^\eta} \left(1 - g(p)\right)\#\mathcal{A} + O(E),$$

where

$$E = \sum_{d<x^\gamma} \left|\#\mathcal{A}_d - g(d)\#\mathcal{A}\right|.$$

One should think of the case when $\mathcal{A}$ satisfies (3.2) with some fixed $\gamma > 0$, and η is taken as a sufficiently small fixed constant. The key point of the fundamental lemma is then that one can still obtain good asymptotic estimates for the number of elements in $\mathcal{A}$ with no prime factors less than z even when z is as large as x^η, provided we have a relatively modest estimate for the distribution of $\mathcal{A}$ in arithmetic progressions.

An immediate consequence is that $\mathcal{A}$ contains $O(\#\mathcal{A}/(\log x)^\kappa)$ primes, and we expect that in most situations this should be the *correct* order of magnitude for the number of primes in $\mathcal{A}$. For example, returning to some of Landau's problems mentioned in Section 1, we find that there are $O(x/(\log x)^2)$ twin primes less than x, and that there are $O(x^{1/2}/\log x)$ prime values of n^2+1 which are less than x, and both estimates are conjectured to be sharp up to the multiplicative constant. We also immediately obtain that $\mathcal{A}$ contains 'many' elements with a bounded number of prime factors as soon as it satisfies something like (3.2). The fact that sieve methods can very flexibly give upper bounds of the right order of magnitude in a wide variety of situations is a very valuable fact when used inside more complicated arguments.

The fundamental lemma essentially produces optimal bounds (with care, the $O_\kappa(e^{-\gamma/\eta})$ error term can usually be handled satisfactorily), and so the sieving process of 'small' primes less than x^η is almost perfect, and as if the small primes were behaving independently of one another. This can therefore also be used just as a preliminary sieving stage, where we first remove all 'small' prime factors $\le x^\eta$ perfectly via an application of the Fundamental Lemma, leaving us to be more careful in trying to handle the about the $O(1/\eta)$ 'large' prime factors (bigger than x^η) of elements of $\mathcal{A}$. Although the behavior of the small primes is essentially that of independence and the same for all sets $\mathcal{A}$ satisfying (3.2), the distribution of the large prime factors in general will vary according to the set. Understanding how much control we have on these large prime factors from (3.2) is still something of a poorly understood art in general, and often the best sieving procedure is tailored to the question at hand.

3.1. Arranging the large prime factors

In general, for any set $\mathcal{A}$ satisfying (3.2), and x sufficiently large we will have that

$$\sum_{\substack{n\in\mathcal{A}\\ p|n\Rightarrow p\geq x^{\eta}}} 1 \leq \big(F(\kappa,\eta,\gamma)+o(1)\big)\#\mathcal{A}\prod_{p\leq x^{\eta}}\big(1-g(p)\big),$$

$$\sum_{\substack{n\in\mathcal{A}\\ p|n\Rightarrow p\geq x^{\eta}}} 1 \geq \big(f(\kappa,\eta,\gamma)+o(1)\big)\#\mathcal{A}\prod_{p\leq x^{\eta}}\big(1-g(p)\big),$$

for some functions $0\leq f(\kappa,\eta,\gamma)\leq F(\kappa,\eta,\gamma)$ depending only on the constant γ in (3.2), the ‘sieve dimension’ κ from (3.1) and η from the sieving threshold of x^{η}.

When $\kappa=1$ (the most common sieving situation) we are in the situation of the ‘linear sieve’, somewhat remarkably we know the optimal values of the functions.

Lemma 6 (Optimality of the linear sieve). *Let g satisfy (3.1) with $\kappa=1$ and $g(p)<1-\epsilon$. Then there are functions $F(s)$, $f(s)$ such that we have the following:*

(1) *For any set $\mathcal{A}$ satisfying (3.2), we have*

$$\sum_{\substack{n\in\mathcal{A}\\ p|n\Rightarrow p\geq x^{\eta}}} 1 \leq \big(F(\gamma/\eta)+o(1)\big)\#\mathcal{A}\prod_{p\leq x^{\eta}}\big(1-g(p)\big),$$

$$\sum_{\substack{n\in\mathcal{A}\\ p|n\Rightarrow p\geq x^{\eta}}} 1 \geq \big(f(\gamma/\eta)+o(1)\big)\#\mathcal{A}\prod_{p\leq x^{\eta}}\big(1-g(p)\big).$$

(2) *There are sets $\mathcal{A}^+,\mathcal{A}^-\subseteq[x,2x]$ which satisfy (3.2) and $g^{\pm}$ which satisfy (3.1) and $g^{\pm}(p)<1-\epsilon$ such that*

$$\sum_{\substack{n\in\mathcal{A}^+\\ p|n\Rightarrow p\geq x^{\eta}}} 1 = \big(F(\gamma/\eta)+o(1)\big)\#\mathcal{A}^+\prod_{p\leq x^{\eta}}\big(1-g^+(p)\big),$$

$$\sum_{\substack{n\in\mathcal{A}^-\\ p|n\Rightarrow p\geq x^{\eta}}} 1 = \big(f(\gamma/\eta)+o(1)\big)\#\mathcal{A}^-\prod_{p\leq x^{\eta}}\big(1-g^-(p)\big).$$

This technical looking statement says that for any $\mathcal{A}$ satisfying a linear sieving problem, we know the optimal upper and lower bounds for the number of sieved elements of the set, based purely on the distribution of $\mathcal{A}$ in arithmetic progressions to modulus x^{γ}. We can take $\mathcal{A}^{\pm}=\{n\in[x,x+x^{\gamma+\epsilon}:\lambda(n)=\mp1\}$ and $g^{\pm}(p)=1/p$, where $\lambda(n)$ is the Liouville function ($\lambda(n)=-1$ if n has an odd number of prime factors, and $\lambda(n)=1$ otherwise) and this gives the functions F, f, which can be written explicitly as solutions to a delay-differential equation. Thus for the basic problem of understanding the consequences of (3.2), we have an essentially complete answer.

Although the linear sieve is essentially optimal, when the sieving dimension is greater than one we have a much poorer understanding of optimality and what we can hope to achieve. The linear sieve bounds are proven using a 'combinatorial sieve', and combinatorial sieves tend to produce the best bounds when κ is reasonably small. When κ gets larger, however, it typically turns out that Selberg's sieve performs better. However, in no circumstance do we have anything like the complete understanding of the picture that we would like.

Question 7. What are the optimal sieve functions for high-degree sieves? What do the extremal sets look like?

For example, the upper bound for the number of prime k-tuplets less than x is larger than the expected truth by $2^k k!$. Although the parity phenomenon would prevent us from obtaining a bound smaller than 2^k times the expected truth, it is very unclear what sort of bound an optimal k-dimensional sieve could hope to prove in this situation. The key innovation in [58] was a new high-dimensional variant of Selberg's sieve tailored to the application at hand, which allowed for notable progress on the sieving problem of bounded gaps between primes (see Section 4). Although this does not appear to help with the direct upper and lower bounds, it indicates that there is potentially a lot left to be understood about high-dimensional sieves.

Question 8. What other arithmetic features of sets $\mathcal{A}$ of interest can be exploited to produce improved sieving bounds?

If there is extra arithmetic information which could distinguish sets $\mathcal{A}$ from extremal sets, this could then be incorporated into the sieving assumptions to hopefully produce better bounds.

For example, Chen's twist [9] was a key innovation used by Chen to show that there are infinitely many primes p with $p+2$ having at most two prime factors, and this exploited the fact that the situation could be viewed as fixing the prime factorization of either n of $n+2$ and viewing it as a sieve problem to produce bounds which are better than what the standard linear sieve would imply. High dimensional sieves often have similar features where they can be viewed as $(k-1)$-dimensional sieving problems or k-dimensional ones, and mixing these perspectives allows one to do slightly better than typical situations [57]. In a different direction, the 'interval sieve' asks for bounds when we know that $\mathcal{A}$ is just an interval – it is known in this case [18, 31] that the optimal sieve functions are closely linked to the presence of Siegel zeros, and so in many situations this limits what we can hope to achieve.

3.2. Limitations of sieve methods and the parity phenomenon

We saw above that the extremal sets $\mathcal{A}^{\pm}$ for the linear sieve were given in terms of numbers with an odd or even number of prime factors. This is an example of a fundamental limitation of sieve methods based purely on arithmetic information of the from (3.2): the parity phenomenon. Roughly, this says that sieve methods cannot distinguish between numbers with an even number of prime factors and an odd number of prime factors.

For example, all sieve upper and lower bounds are based on using sieve weights which are short divisor sums

$$w_n = \sum_{\substack{d|n\\ d<x^\gamma}} \lambda_d.$$

Thus, recalling that $\lambda(n) = -1$ if n has an odd number of prime factors, and $\lambda(n) = 1$ otherwise, we see

$$\sum_{n\in\mathcal{A}} w_n\Big(\frac{1\pm\lambda(n)}{2}\Big) = \frac{1}{2}\sum_{n\in\mathcal{A}} w_n + O\Big(\sum_{d<x^\gamma}|\lambda_d|\Big|\sum_{\substack{n\in\mathcal{A}\\ d|n}}\lambda(n)\Big|\Big).$$

For most sets $\mathcal{A}$ of interest, it is believed that the inner sums on the right-hand side should always be very small, meaning that the same total weight is put on numbers with an even number of prime factors as those with an odd number of prime factors (although actually proving this is almost as hard as proving an asymptotic formula for primes in $\mathcal{A}$).

Because the weight is equidistributed between numbers with an even and an odd number of prime factors, it means that any upper bound sieve for primes will be off by a factor of at least 2 (the weight placed upon primes can be at most the total weight of numbers with an odd number of prime factors, which in turn is at most half the total weight). It also means that we cannot hope to obtain a nontrivial lower bound for the number of primes in a set $\mathcal{A}$ by just using pure sieve methods.

In various situations, this elementary loss of a factor of 2 from sieve methods is intimately linked to the possible presence of Siegel zeros (which would cause certain residue classes to have double the expected number of primes of a certain size.) For example, the Brun–Titchmarsh Theorem [69] (proven using sieve methods) states that

$$\pi(x;q,a) \le \frac{2x}{\varphi(q)\log(x/q)}.$$

When x is fairly large relative to q, this is off by a factor of roughly 2 from the expected asymptotic, but improving the constant 2 to $2-\delta$ in this regime would rule out the possibility of a Siegel zero.

4. SIDE-STEPPING LIMITATIONS OF SIEVE METHODS

Although sieve methods alone cannot directly produce primes, sometimes this apparent limitation can be sidestepped. For example, consider the following result ([58, 59, 71, 82] and unpublished work of Tao).

Theorem 9 (Bounded gaps between primes). *Let k be a positive integer. Then*

$$\liminf_n (p_{n+k} - p_n) < \infty.$$

In the special case when $k = 1$, we can take the finite constant to be 246; for general k, we can take the bound to be $O(e^{3.815k})$ thanks to work of Baker–Irving [3].

This result manifestly says something about prime numbers, but ultimately only relies on arithmetic information of the form (3.2), in this case the Bombieri–Vinogradov

Theorem. The reason this result isn't prevented from saying something by the parity phenomenon is because it sidesteps some of the issues via the pigeonhole principle, which then avoids the need to specify exactly which quantities are taking prime values. More specifically, the proof of Theorem 9 relies on considering the quantity

$$S = \sum_{n\sim x}\left(\sum_{i=1}^{K}\mathbf{1}_{\mathbb{P}}(n+h_i) - k\right)w_n$$

for some suitable fixed constants $h_1 < \cdots < h_K$ (chosen such that $\prod_{i=1}^{K}(n+h_i)$ is not always a multiple of a fixed prime p) and some nonnegative sieve weight w_n tailored to the situation at hand. Since $w_n \ge 0$, showing that $S > 0$ implies that there is some $n \sim x$ for which at least $k+1$ of $n+h_1,\dots,n+h_K$ are simultaneously prime, and hence there are $k+1$ primes all contained in an interval of length $h_K - h_1$. The fact that we do not have any control over *which* of the different $n+h_i$ are prime, merely the fact that several of them are prime is what allows us to sidestep the parity phenomenon issue.

Another example of proving the existence of primes in a set by sidestepping the usual obstacles is due to Elkies [15].

Theorem 10 (Elkies' Theorem). *Let $E/\mathbb{Q}$ be an elliptic curve. Then there are infinitely many supersingular primes for E.*

The proof actually only relies on Dirichlet's theorem on primes in arithmetic progressions; all the nontrivial content of the proof is showing that there are polynomials P_ℓ encoding E_p having complex multiplication by a suitable order (this happens if p divides the numerator of $P_\ell(j(E))$ and $-\ell$ is a quadratic nonresidue $\pmod p$). Carefully choosing a sequence of ℓ's then shows that there must be infinitely many distinct such p's. Thus this is an example where we started with what seemed a difficult counting problem, but by focusing on a special subsequence we were able to reduce to a much counting problem for primes.

One result about primes which relies on sieving procedures but is not directly limited by the parity phenomenon is that of large gaps between primes. In this case it is again fruitful to focus on a special case; if we have a long string of consecutive integers $n, n+1,\dots,n+y$ all with a small prime factor $\le (\log n)/2$, then certainly we have a long gap between primes. The fact we only search for factors $\le \log n$ limits our approach (we expect we cannot find gaps between primes less than x bigger than $(\log x)(\log\log x)^{2+o(1)}$ in this way), but enables us to understand the situation by looking at n in residue classes $(\bmod \prod_{p\le(\log x)/2} p)$, and choosing a convenient residue class to make all the consecutive integers composite. This indirect approach therefore allows us to avoid directly counting primes. The current record is [19,20,60]

Theorem 11 (Large gaps between primes).

$$\sup_{p_n\le X}(p_{n+1}-p_n) \gg \frac{(\log x)(\log\log x)(\log\log\log\log x)}{\log\log\log x},$$

This improves upon an old bound of Erdős–Rankin [17,72]. The key input for this bound was a version of Theorem 9 showing the existence of certain residue classes containing unusually many small primes – this exploited the fact that sieve results (when successful) are often very flexible and uniform with respect to other parameters.

The parity phenomenon issue applies equally to estimating primes or estimating sums involving the Liouville function $\lambda(n)$. It is therefore somewhat remarkable that Tao [74] was able to avoid this for the 2-point Chowla conjecture.

Theorem 12 (Logarithmically average 2-point Chowla).

$$\sum_{n<x} \frac{\lambda(n)\lambda(n+1)}{n} = o(\log x).$$

The key property that is exploited here is the multiplicativity of λ; by using $\lambda(np) = -\lambda(n)$ and averaging over small primes p, the problem is turned from a binary problem (which we might expect to be limited by the parity phenomenon) to a ternary one (where we might hope to use a version of the circle method and not be limited by the parity phenomenon). Unfortunately, the subsequent steps appear only able to handle very small primes p, which appears to stop this idea applying to questions about the primes.

5. PRIMES IN ARITHMETIC PROGRESSIONS AND EXTENDING THE LEVEL OF DISTRIBUTION

Most results using sieve methods rely crucially on an estimate of the form (3.2), and the strength of the final results is determined by how large we can take the constant γ to be. Natural questions are how far we can push the constant γ for a given set $\mathcal{A}$, and whether we really need the full strength of (3.2) or whether we can produce a weaker, but more technical result which would still suffice for intended applications.

How far we can extend these estimates naturally depends on the particular set $\mathcal{A}$ in question. For simplicity, we will focus on the case when $\mathcal{A}$ is closely related to the set of primes ($\mathcal{A}$ could be shifted primes, like in the Twin Prime problem, for example) since this is a common case which appears regularly. In this situation, (3.2) is asking us to understand primes in arithmetic progressions, and typically the basic tool used is the Bombieri–Vinogradov Theorem [4,77].

Theorem 13 (Bombieri–Vinogradov Theorem). *Let $\epsilon, A > 0$. Then we have*

$$\sum_{q \le x^{1/2-\epsilon}} \sup_{(a,q)=1} \left| \pi(x;a,q) - \frac{\pi(x)}{\varphi(q)} \right| \ll_{\epsilon,A} \frac{x}{(\log x)^A}.$$

This asserts that the set of primes shifted by a constant satisfies a strong form of (3.2) for any $\gamma < 1/2$. From the point of view of sieve methods (where we typically only need estimates 'on average' over arithmetic progressions) this is typically an unconditional substitute for the Generalized Riemann Hypothesis. We expect, however, that one should be able to go much further [16].

Conjecture 1 (Elliott–Halberstam Conjecture). *Let $\epsilon, A > 0$. Then we have*

$$\sum_{q \le x^{1-\epsilon}} \sup_{(a,q)=1} \left| \pi(x;q,a) - \frac{\pi(x)}{\varphi(q)} \right| \ll_{\epsilon,A} \frac{x}{(\log x)^A}.$$

Increasing the arithmetic information available to the sieve method in question naturally produces stronger results; under the Elliott–Halberstam conjecture. For example, the bound 246 of the case $k = 1$ of Theorem 9 can be improved to 12 [58], and we can obtain an upper bound for twin primes which is a factor of only 2 larger than the expected truth.

Unfortunately in this formulation we do not know how to extend the Bombieri–Vinogradov Theorem to moduli beyond $x^{1/2}$ – this is often known as the 'square-root barrier', and the difficulty of the problem increases dramatically at this point where it goes beyond the region of the Generalized Riemann Hypothesis. However, if we ask for a slightly more technical version of these results on primes in arithmetic progressions, then one *can* do better. The pioneering work of Fouvry and Bombieri–Friedlander–Iwaniec [5–7,22] produced various results accounting for moduli as large as $x^{4/7-o(1)}$. This was recently extended [64] to larger moduli still.

Theorem 14 (Beyond $x^{1/2}$ barrier for nice coefficients). *Let $\lambda(n)$ be 'triply well factorable' and $\epsilon, A > 0$. Then we have*

$$\sum_{q \le x^{3/5-\epsilon}} \lambda(q) \left(\pi(x;q,a) - \frac{\pi(x)}{\varphi(q)} \right) \ll_{a,\epsilon,A} \frac{x}{(\log x)^A}.$$

For simplicity we will not go into the precise definition of 'triply well factorable' (it roughly means that $\lambda(q)$ can be decomposed into a triple-convolution of sequences of any predetermined sizes). The key point here is that one can take any $\gamma < 3/5$ so we can consider very large moduli, and at the same time the technical weakenings (triply well factorable sequences and a dependency on the residue class) are sufficient for various applications to sieve methods. For example, Iwaniec [45] showed that the linear sieve weights can be modified to become 'well-factorable,' which then makes linear sieve estimates amenable to such results. Working a bit harder, one can show that the linear sieve weights then cancel with the error term for primes in arithmetic progressions up to moduli of size $x^{7/12-\epsilon}$. Moreover, recent work of Lichtman [51] shows one can modify the linear sieve construction itself to exploit newer equidistribution results profitably (the linear sieve is only optimal at exploiting the information (3.2)).

The spectacular work of Zhang [82] on bounded gaps between primes was an important application of breaking the square-root barrier (even though now we do not need such strong results to prove bounded gaps between primes), and similarly the work of Adleman–Fouvry–Heath-Brown [1,23] on Fermat's last Theorem relied crucially on ideals going beyond the $x^{1/2}$ barrier (although now we know Fermat's Last Theorem in full [75,80].) Even in the absence of a headline application, it still feels a fundamental and central problem in analytic number theory to concretely go beyond the Bombieri–Vinogradov range.

Question 15. Can we show for any a, A,

$$\sum_{\substack{q \leq x^{1/2+\delta} \\ (q,a)=1}} \left| \pi(x; q, a) - \frac{\pi(x)}{\varphi(q)} \right| \ll_{a,A} \frac{x}{(\log x)^A}$$

for some fixed $\delta > 0$?

The work of Bombieri–Friedlander–Iwaniec [5–7] covered most terms which occur when performing a combinatorial decomposition of the primes, leaving one only to deal with products of j integers of size roughly $x^{1/j}$ for $j \in \{4, 5, 6\}$. The recent work [63] handles the case $j = 5$, but only obtains partial results for $j = 4$ and $j = 6$, which remain to be handled. In particular, we highlight the case $j = 4$, which appears to clearly need new ideas

Question 16. Can one obtain a nontrivial estimate for

$$\sum_{q \leq x^{1/2+\delta}} \left| \sum_{\substack{n_1,n_2,n_3,n_4 \in [x^{1/4}, 2x^{1/4}] \\ (n_1n_2n_3n_4, q)=1}} \left(\mathbf{1}_{n_1n_2n_3n_4 \equiv 1 \pmod{q}} - \frac{1}{\varphi(q)} \right) \right| ?$$

6. BILINEAR ESTIMATES

Although basic sieve methods relying only on information about $\mathcal{A}$ in arithmetic progressions cannot detect primes because of the parity barrier, it is known that if you incorporate extra 'bilinear' information into the method, then you can count primes; this ultimately goes back to the pioneering work of Vinogradov [78]. For example, by inclusion–exclusion on the largest prime factor, for $\mathcal{A} \subseteq [x, 2x]$, we have

$$\#\{p \in \mathcal{A}\} = S(\mathcal{A}, z) - \sum_{z < p < x^{1/2}} S(\mathcal{A}_p, p).$$

When z is a small power of x, basic sieve methods can get good upper and lower bounds for $S(\mathcal{A}, z)$. The sum over primes counts products $pm \in \mathcal{A}$ where p and m are both larger than z, and the power of bilinear sums is that they can estimate the number of such products in $\mathcal{A}$ with very little arithmetic information required beyond that both factors are of moderate size.

To state things more precisely, it is often easiest to compare the set $\mathcal{A}$ of interest with a simpler set $\mathcal{B}$ where we know how to count primes using techniques from multiplicative number theory, but which is expected to have similar distributional properties. For example, if $\mathcal{A} = [x, x + x^\theta]$ is a short interval, then we might take $\mathcal{B} = [x, x + x\exp(-\sqrt{\log x})]$ to be a long interval. A slight extension of (3.2) is then

$$\sum_{m \sim M} \alpha_m \sum_{n \in \mathcal{I}} \left(\mathbf{1}_{nm \in \mathcal{A}} - \frac{\#\mathcal{A}}{\#\mathcal{B}} \mathbf{1}_{nm \in \mathcal{B}} \right) \ll_A \frac{\#\mathcal{A}}{(\log x)^A} \tag{6.1}$$

for any 1-bounded sequence α_m, constant A, interval $\mathcal{I}$, and any $M < x^\gamma$. With this formulation, we can consider similar variants, in particular the estimate

$$\sum_{m \sim M} \sum_{n} \alpha_n \beta_m \left(\mathbf{1}_{nm \in \mathcal{A}} - \frac{\#\mathcal{A}}{\#\mathcal{B}} \mathbf{1}_{mn \in \mathcal{B}} \right) \ll_A \frac{\#\mathcal{A}}{(\log x)^A} \tag{6.2}$$

for all 1-bounded sequences α_n, β_m.

We call (6.1) a 'Type I' estimate, and (6.2) a 'Type II' or 'bilinear' estimate for $\mathcal{A}$.

One should interpret condition (6.2) as saying that we can obtain an asymptotic formula for products with some prescribed prime factorization, provided these factorizations always contain a divisor of a convenient size.

Naturally, (6.2) is typically much harder to establish, and proving a nontrivial Type II estimate is normally the key technical difficulty which needs to be overcome if wanting to prove the existence of primes in some set $\mathcal{A}$. For example, we would like to establish fairly good Type I estimates for the sets mentioned in the introduction, but we currently do not know how to estimate Type II sums for most of the outstanding open problems on primes.

Question 17 (Type II estimates for twin primes). Can one estimate a Type II sum associated to Twin Primes such as

$$\sum_{n\sim N}\sum_{m\sim M}\alpha_n\beta_m\Lambda(nm+2)$$

for arbitrary 1-bounded sequences α_n,β_m?

One might also try to reduce both prime variables to bilinear terms, but sums such as

$$\sum_{n\sim N}\sum_{\substack{m\sim M\\ nm+2=rs}}\sum_{r\sim R}\sum_{s\sim S}\alpha_n\beta_m\gamma_r\delta_s$$

also appear infeasible to handle. (The natural Cauchy–Schwarz argument leads to conditions like $n_1s_2-s_2n_1=d$ for some $d|2n_2-2n_1$, and little appears to have been gained.)

Note that (6.2) cannot be expected to hold if $\mathcal{A}$ has a lot of multiplicative structure in the sense that information about n tells us a lot about which m's can have $nm\in\mathcal{A}$. This is to be expected – if $\mathcal{A}$ contained only numbers with an even number of prime factors, for example, then we could not hope to produce primes and so we expect that we cannot produce good Type II estimates. In this case the parity of the number of prime factors of n would dictate the parity of the number of prime factors of m, and so by choosing α_n,β_m to account for these we would give a counterexample to the bound (6.2). Indeed, (6.2) can be thought of as ruling out such multiplicative conspiracies, so that the arithmetic nature of n and m over products $nm\in\mathcal{A}$ is being 'independent on average'.

Although (6.2) is ruling out a certain amount of multiplicative structure within $\mathcal{A}$, somewhat perversely we are typically only able to estimate Type II terms effectively if $\mathcal{A}$ has some different multiplicative structure which we are able to exploit to show that the factors n,m behave somewhat independently of one another. For example, after some initial massaging one typically attempts to prove a Type II estimate via Cauchy–Schwarz to eliminate one of the unknown sets of coefficients (there is typically little lost in doing this, since we cannot rule out $\alpha_n=\operatorname{sgn}(\sum_m\beta_m\mathbf{1}_{nm\in\mathcal{A}})$), leaving us to estimate a quantity like

$$\#\{n\sim x/M : m_1n\in\mathcal{A}, m_2n\in\mathcal{A}\}. \tag{6.3}$$

If we can estimate this quantity reasonably accurately (and the diagonal terms with $m_1=m_2$ do not dominate), then we should be optimistic of obtaining a Type II estimate. It is precisely the difficulty of estimating quantities like (6.3) which limits our ability to apply Type I/II methods.

6.1. Type I/II ranges to primes

We first introduce some general notation to talk about sets where we can estimate the bilinear Type II sums in certain ranges at least.

Definition (Type I/II ranges). Given $\mathcal{A}, \mathcal{B} \subseteq [x, 2x]$:

- We say that $\mathcal{A}$ satisfies a Type I range of $[0, \gamma]$ if (6.1) holds for all choices of $M \le x^\gamma$ (for all $A > 0$, all intervals $\mathcal{I}$ and all 1-bounded sequences α_m).
- We say that $\mathcal{A} \subseteq [x, 2x]$ satisfies a Type II range of $[\alpha, \beta]$ if (6.1) holds for all choices of $M \in [x^\alpha, x^\beta]$ (for all $A > 0$ and all 1-bounded sequences α_m, β_n).

We typically suppress mentioning $\mathcal{B}$, since we assume that $\mathcal{B}$ is a simple set like $[x, 2x]$ in which we can count primes well.

Since we think of $\mathcal{A} \subseteq [x, 2x]$, we see that by switching the roles of n, m if $\mathcal{A}$ satisfies a Type II range of $[\alpha, \beta]$ then it also has a Type II range of $[1 - \beta + \epsilon, 1 - \alpha - \epsilon]$ for any $\epsilon > 0$.

A key basic result, is that if we have 'enough' Type I/II arithmetic information, then we can count primes in $\mathcal{A}$.

Lemma 18 (Vaughan's identity). *Let $\mathcal{A}$ satisfy a Type I range of $[0, \gamma]$ and a Type II range of $[\alpha, \alpha + \beta]$. If $\beta + \gamma > 1$ then we have*

$$\#\{p \in \mathcal{A}\} = \frac{\#\mathcal{A}}{\#\mathcal{B}} \#\{p \in \mathcal{B}\}\big(1 + o(1)\big).$$

(This formulation is somewhat different from typical statements of Vaughan's identity. Ignoring some minor technical considerations to do with separating variables and removing log-coefficients, it follows from choosing $U = x^\alpha$, $V = x^{1-\alpha-\beta}$ in [11, CHAPTER 24], for example.)

Therefore, if the length of the Type I range plus the length of the Type II range is bigger than 1, we can obtain an asymptotic formula for primes in $\mathcal{A}$. Unfortunately, if $\mathcal{A}$ satisfies some Type I/II estimates but the combined lengths are not bigger than 1, we cannot necessarily obtain an asymptotic formula for primes and the precise Type I/II regions when we can produce primes becomes a more subtle arithmetic-combinatorial question.

Although we are only considering sets $\mathcal{B}$ which are 'simple' (and so contain many primes), essentially the same arguments allow us to show that conclusions of Lemma 18 hold even if $\mathcal{B}$ is a more complicated set. Thus in principle these techniques can show different sets $\mathcal{A}, \mathcal{B}$ contain the roughly same number of primes, even if we are unable to establish precisely how many primes there are in either set. In this way the results are 'independent' of the Prime Number Theorem, but are not 'producing' primes.

For many applications, we merely wish to prove the existence of primes in $\mathcal{A}$. Therefore even if we do not have sufficient Type I/II ranges to obtain an asymptotic formula, we might still be able to obtain a nontrivial lower bound for the number of primes in $\mathcal{A}$. Methods to do this were gradually developed [39,46] culminating in Harman's sieve [35]. This allowed one to exploit positivity to drop inconvenient terms and obtain a lower bound of the correct order of magnitude, provided one still had suitably large Type I and Type II ranges. Given this, the strategy for proving the existence of primes in $\mathcal{A}$ then becomes the following:

(1) Establish a Type I estimate in as large a range as possible;

(2) Establish a Type II estimate in as large a range as possible;

(3) Use a sieve decomposition to verify the Type I/II information established is sufficient to obtain a non-trivial lower bound for primes in $\mathcal{A}$.

With this is mind, we define the upper and lower bound functions $L(\alpha,\beta,\gamma)$ and $U(\alpha,\beta,\gamma)$, obtained from an optimal translation of this arithmetic information.

Definition (Optimal constants in Harman's sieve). For given fixed constants $\alpha,\beta,\gamma\in[0,1]$, and $\mathcal{B}=[x,2x]$:

- Let $L_x(\alpha,\beta,\gamma)$ denote the infimum of $\pi(\mathcal{A})\log x/\#\mathcal{A}$ over all sets $\mathcal{A}\subseteq[x,2x]$ satisfying a Type I range $[0,\gamma]$ and a Type II range $[\alpha,\alpha+\beta]$. Let $L(\alpha,\beta,\gamma)=\liminf_{x\to\infty}L_x(\alpha,\beta,\gamma)$.
- Let $U_x(\alpha,\beta,\gamma)$ denote the supremum of $\pi(\mathcal{A})\log x/\#\mathcal{A}$ over all sets $\mathcal{A}\subseteq[x,2x]$ satisfying a Type I range $[0,\gamma]$ and a Type II range $[\alpha,\alpha+\beta]$. Let $U(\alpha,\beta,\gamma)=\limsup_{x\to\infty}U_x(\alpha,\beta,\gamma)$.

Clearly, $0\le L(\alpha,\beta,\gamma)\le U(\alpha,\beta,\gamma)$. Moreover, assuming that $\gamma>0$, we have that $U(\alpha,\beta,\gamma)\ll 1$ from Lemma 5. If $\gamma>1/2$ then we know that $L(\alpha,\beta,\gamma)$ and $U(\alpha,\beta,\gamma)$ will be continuous functions on $[0,1]^3$; we expect them to be piecewise smooth and continuous everywhere.

In many problems, we are most interested in showing the existence of primes in $\mathcal{A}$, which would follow if $\mathcal{A}$ satisfied (6.1) and (6.2) for some α,β,γ such that $L(\alpha,\beta,\gamma)>0$. Therefore a crucial open question is the following.

Question 19. For which choices of α,β,γ do we have $L(\alpha,\beta,\gamma)>0$?

The machinery of Harman's sieve allows one to compute a numerical lower bound for $L(\alpha,\beta,\gamma)$ (or an upper bound for $U(\alpha,\beta,\gamma)$) for given constants α,β,γ in terms of various multidimensional integrals, but the lower bound is not guaranteed before time to be positive. It is slightly unsatisfying that the computations often have to rely on a moderate amount of explicit numerical calculation of integrals and the decompositions need to be done by hand, but empirically this typically works well. If one has a moderately large constant γ for the Type I range, then in practice we can often succeed in showing a positive lower bound even when β is as small as $1/20$ or $1/30$, and often (but not always) an argument which produces a nontrivial Type II range will produce one of an adequate length. It is the empirical fact that one can get a nontrivial lower bound via Harman's sieve even with quite limited Type II ranges which makes it very applicable.

That said, it would be desirable to have a much better understanding of the optimal ways to apply Harman's sieve, the optimal constants which come out, and what sort of sets we would need to distinguish ourselves from if we wanted to produce stronger results.

Question 20. Given constants α, β, γ, what are the optimal values $L(\alpha, \beta, \gamma)$ and $U(\alpha, \beta, \gamma)$? What are the sets which achieve these maxima and minima?

Work-in-progress [21] makes some first steps to understanding optimality in Harman's sieve, but the general picture appears to be arithmetically quite subtle (much more so than for the linear sieve bounds) and combinatorially quite involved.

If we have some nontrivial arithmetic information about $\mathcal{A}$, but we know that $\mathcal{A}$ does not contain the expected number of primes, then we know that this must be compensated by $\mathcal{A}$ also containing a different number of products of r primes, for some small value of r.

7. PRIMES IN THIN SETS

One particularly challenging situation which encompasses many important situations is when the set $\mathcal{A}$ in question contains $O(x^{1-\theta})$ elements in $[x, 2x]$ for some fixed $\theta > 0$. In this case $\mathcal{A}$ is a sparse subset of the integers, and there are limitations on what sort of Type I and Type II information one could hope to establish even in the most optimistic scenarios.

Trivially, $\#\mathcal{A}_d$ is an integer, and so we can only hope for the approximation $\#\mathcal{A}_d \approx g(d)\#\mathcal{A}$ to be accurate when $d < \#\mathcal{A}$, which limits our Type I range to $\gamma \leq 1 - \theta$. Similarly, for typical $n \sim N$ there should be roughly $\#\mathcal{A}/N$ choices of $m \sim x/N$ with $mn \in \mathcal{A}$, and so we can only hope to obtain a nontrivial estimate for $\sum_{m:mn\in\mathcal{A}} \beta_m$ if $N < \#\mathcal{A}$. This limits our Type II range to $\alpha \geq \theta$. Finally, if we attempt to estimate our Type II sums by following the standard Cauchy–Schwarz strategy of estimating

$$\#\{n \sim N : m_1 n \in \mathcal{A}, m_2 n \in \mathcal{A}\}, \tag{7.1}$$

then (for generic m_1, m_2) we would expect this count to be roughly $N\#\mathcal{A}^2/x^2$. For this to be typically greater than 1, this would limit us to $N > x^2/\mathcal{A}^2 = x^{2\theta}$, and so $\alpha + \beta < 1 - 2\theta$ in our Type II range. Thus if $\mathcal{A} \subseteq [x, 2x]$ with $\#\mathcal{A} = x^{1-\theta}$, in the absence of more sophisticated methods we expect to be limited to a Type I range of $[0, x^{1-\theta}]$ and a Type II range of $[x^{\theta}, x^{1-2\theta}]$. In particular, this range would be sufficient to obtain an asymptotic formula via Vaughan's identity if $\#\mathcal{A} > x^{3/4}$, but we would expect to fail to obtain any Type II information at all if $\#\mathcal{A} < x^{2/3}$.

In various favorable situations we can obtain Type I and Type II estimates of this strength.

(1) Let $\mathcal{A} = \{n \sim x : \|\alpha n + \beta\| < n^{-\theta}\}$ for given irrationals α, β, corresponding to the question of inhomogeneous Diophantine approximation by primes. In this

situation, $\#\mathcal{A} = x^{1-\theta+o(1)}$ and it follows from work of Vaughan [76] that one can obtain a Type I range $[0, 1-\theta]$ and a Type II range $[\theta, 1-2\theta]$, therefore covering essentially the full range.

(2) Let $N(x_1 + x_2\sqrt[n]{a} + \cdots + x_{n-k}\sqrt[n]{a^{n-k-1}})$ be the incomplete norm form associated to the Kummer extension $\mathbb{Q}(\sqrt[n]{a})$, and $\mathcal{A}$ be the value set of N on $[1, x^{1/n}]^n$. Since N is a degree n polynomial in $n-k$ variables, $\mathcal{A}$ contains roughly $x^{1-k/n}$ in $[x, 2x]$ and so is a thin set of integers. In [62] we obtain a Type I range $[0, 1-k/n]$ and a Type II range $[k/n, 1-2k/n]$, therefore corresponding to the optimistic basic estimates above.

Jia [48] showed that if $\theta < 9/28$ then Harman's sieve can produce a lower bound of the correct order of magnitude for the number of primes in a set $\mathcal{A}$ satisfying a Type I estimate $[0, 1-\theta]$ and a Type II estimate $[\theta, 1-2\theta]$.

In some situations one can exploit extra structure of the problem to obtain slightly wider Type II estimates. One might hope to obtain cancellations in the error terms $E(m_1, m_2)$ occurring in estimating $\#\{n \sim N : m_1 n \in \mathcal{A}, m_2 n \in \mathcal{A}\}$, for example, which might allow one to have a Type II range beyond $1-2\theta$.

(1) Let $\mathcal{A} = \{n \in [x, x + x^{1-\theta}]\}$, so we are investigating primes in short intervals. In Section 2 we saw that we can use zero-density methods to obtain an asymptotic formula for $\theta < 5/12$ (note that $5/12 > 1/3$, so this is much sparser than the examples above). By using Dirichlet polynomials, we can actually obtain nontrivial arithmetic information for this problem whenever $\theta > 1/2$ (although we can only obtain Type II style estimates for coefficients of special types corresponding to convolutions of 3 rather than 2 sequences). By combining these estimates for triple convolutions (and more) with Harman's sieve we can unconditionally show the existence of primes in intervals $[x, x + x^{0.525+o(1)}]$ [2], which is only an exponent only slightly worse than what we would obtain under the Riemann Hypothesis. The most powerful arithmetic input is Watt's mean value Theorem [79] – it would be very desirable to have some new arithmetic estimates which could apply to these short interval problems, but currently our techniques do not seem able to go beyond Watt's work.

(2) Let $\mathcal{A} = \{a^3 + 2b^3 : a, b < x^{1/3}\}$. After switching to prime ideals, Heath-Brown [38] is essentially able to classify those m_1, m_2 for which there is an n with $m_1 n, m_2 n \in \mathcal{A}$ since such n can be given explicitly in terms of m_1, m_2, and then obtain suitable cancellations over these special pairs m_1, m_2. This enables him to obtain a Type II range $[1/3, 1/2]$, which is sufficient for obtaining an asymptotic formula for primes represented by $a^3 + 2b^3$, even though this only contains roughly $x^{2/3}$ elements in $[1, x]$. Li [50] is able to generalize this to further restrict b to be small, allowing him to handle sets even sparser than this.

(3) Let $\mathcal{A} = \{n \sim x : \|\alpha n\| < x^{-1/3+\epsilon}\}$. Then $\mathcal{A}$ contains roughly $x^{2/3+\epsilon}$ integers of size x, but nevertheless Matomäki [53] (building on [40]) was able to show that $\mathcal{A}$ still contained primes by establishing nontrivial arithmetic information in wider ranges. Again, to establish these wider ranges she needed to consider trilinear sums.

In a slightly different direction in [61] Type II estimates were deduced by exploiting a very nice Fourier structure in the underlying set. This is an example where the set does not have obvious 'linear structure' (such as short intervals, or the distribution of αn modulo one), and does not lack obvious multiplicative structure which makes it more feasible to estimate (7.1), but nevertheless nontrivial arithmetic information can be established (in this case within the Hardy–Littlewood circle method). It would be interesting to add to this example.

We mention in passing the recent work of Heath-Brown–Li [41] on primes of the form $X^2 + p^4$ and Merikoski [67] on $X^2 + (Y^2 + 1)^2$ and Xiao [81] on primes of the form $f(a, b^2)$ for binary quadratic forms f all generalizing the work of Friedlander–Iwaniec on $X^2 + Y^4$ [27].

Even with these proof-of-concept results that in principle one can establish some sort of nontrivial arithmetic information with fairly general coefficient sequences in some sparse sets, all approaches seem to break down completely when considering sets containing fewer than $x^{1/2}$ elements in $[x, 2x]$.

Question 21. Is there a plausible way to adapt Type I/II machinery to apply to very sparse sets with $x^{1/2-\epsilon}$ elements in $[x, 2x]$?

Without some advance in this direction, we do seem to have any means of counting primes in intervals of length smaller than $x^{1/2}$, and thereby addressing Legendre's conjecture on the existence of a prime between consecutive squares. Of course, we expect there to be primes in much shorter intervals (as short as $(\log x)^{2+o(1)}$), but going beyond $x^{1/2}$ seems out of reach for now, even if we assume the Riemann Hypothesis and things like Montgomery's Pair Correlation Conjecture [68].

8. FURTHER ARITHMETIC INFORMATION

Even if the Type I/Type II arithmetic information in insufficient for generating primes (or asymptotic formulae for primes), we can sometimes remedy the situation by incorporating further arithmetic information into the method.

For example, we mentioned in Section 7 that for the problem of primes in short intervals or for small values of αp modulo one it was important that there was additional flexibility to consider triple convolutions of sequences, rather than just bilinear sums. Often we find that the size of factors of terms produced in a decomposition of the primes is the key feature – when terms factor in a convenient manner one can produce much stronger results.

As well as higher order convolutions (corresponding to assuming some factorization properties of the sequences α_n or β_m) we can also exploit the fact that sometimes we are able to produce stronger results if some of the sequences involved are just the constant 1. For example, we have Linnik's identity [52]

$$\frac{\Lambda(n)}{\log n} = -\sum_{j=1}^{\infty} \frac{(-1)^j}{j} \tau_j'(n)$$

where $\tau_j'(n)$ counts representations of n as the product of j integers all bigger than 1. In principle this allows us to understand primes in $\mathcal{A}$ by understanding the average of $\tau_j'(n)$ for $n \in \mathcal{A}$. Understanding $\tau_j'(n)$ is similar to understanding j-fold convolutions in $\mathcal{A}$, therefore generalizing our linear and bilinear sums. Moreover, in this formulation the coefficients of each of the j factors is just 1 rather than some unknown sequence. This additional flexibility of only needing to consider smooth coefficient sequences is difficult to exploit unless some of the variables are very long like in the case of Type I estimates (and for practical applications Heath-Brown's identity [36] is often more convenient to use), but is crucial in some situations. For example, the recent work [63–65] on primes in arithmetic progressions crucially relied on estimates for the divisor function in arithmetic progressions and for $\tau_3(n)$ in arithmetic progressions [24,25,37].

One further comment is that the coefficients which naturally occur from Buchstab iterations are the indicator function of products of primes, where each prime is of a roughly fixed size. This means that rather than requiring estimates like (6.2) for arbitrary sequences, we only really require this when α_n and β_m look like the indicator function of primes, or products of primes. In the ground-breaking work of Friedlander–Iwaniec on $X^2 + Y^4$ representing primes [26,27] the fact that the coefficients satisfied a suitable Siegel–Walfisz Theorem was crucial, and so the Type II estimates were only valid for this reduced class of coefficients.

One simple observation is that $\tau_j(n)$ are the coefficients of the degree j L-function $\zeta(s)^j$. There is a general principle that often estimates which can be obtained in a direct manner for $\tau(n)$ can be also obtained in a more complicated manner for the Fourier coefficients of suitable cusp forms via the spectral theory of automorphic forms. It is therefore compelling to speculate whether this would allow for further 'higher degree' arithmetic information to be incorporated.

Question 22. Can one use coefficients of other higher degree L-functions to aid counting primes?

Work of Drappeau–Maynard [14] made crucial use of the Sato–Tate distribution of Kloosterman sums to enable an estimation of a sum over primes, where arithmetic properties of the underlying sequence essentially reduced the sieve dimension. Since Fourier coefficients have similar distributional features, one might hope that this simple example could be indicative of a wider approach.

9. CHOICE OF LIFT AND COMPARISON SETS

When attempting to count primes in $\mathcal{A}$ using the Type I/II sums strategy, one wants to understand a sum

$$\sum_{p\in\mathcal{A}} a_p$$

over *primes*, and we study this by gaining arithmetic information (such as Type I/II estimates) for a sequence a_n over *integers* $n \in \mathcal{A}$. We therefore choose a *lift* of the sequence a_p supported on primes to the sequence a_n supported on integers which hopefully is more amenable to estimation. In many contexts there is a natural choice of a_n which works well (e.g., $a_p = 1$ and $a_n = 1$), but one could imagine other choices also being worthy of consideration (or perhaps multiple different lifts). For example, if one could understand the sums with $a_n = 2/\tau(n)$, then one would have a lift of the sequence $a_p = 1$ which would remain closer to the primes, and it would be correspondingly easier to detect primes given the same basic arithmetic information (it would be reducing the sieve dimension). So far our estimates appear to have been limited to the simplest possible choices, but it is natural to ask if this is really necessary.

Question 23. Are there situations where other lifts a_n of the sequence a_p can aid estimating primes?

As a very basic proof-of-concept, in some situations it is easier to lift $a_p = 1$ to $a_n = \theta(n)$ where $\theta(n)$ is a sieve weight ensuring that a_n behaves as if it is supported only on small prime factors. But ideally we would find a nontrivial way to lift to a sequence sensitive to all prime factors of n, not just small ones.

In (6.1) and (6.2) we compare arithmetic counts in a set $\mathcal{A}$ to a simpler set $\mathcal{B}$, but the choice of $\mathcal{B}$ is left to the application at hand. In most cases $\mathcal{B}$ is a truly simple set (such as an interval) where something like the Prime Number Theorem can be applied directly. However, in some cases it is advantageous (or important) to have more complicated comparison sets (or one could generalize to a weighted sequence). For example, in looking at primes in arithmetic progressions to large moduli, it is useful to compare the indicator function of the residue class $\mathbf{1}_{n\equiv a \pmod{q_1q_2}}$ *not* with the basic choice of 1 (or $\mathbf{1}_{(n,q_1q_2)=1}$), but with the 'intermediate complexity' sequences $\mathbf{1}_{n\equiv a \pmod{q_1}}$. This allows us to use additive Fourier analysis to show that $\mathbf{1}_{n\equiv a \pmod{q_1q_2}} \approx \mathbf{1}_{n\equiv a \pmod{q_1}}$ in some average sense, and then use multiplicative Fourier analysis (Dirichlet characters) to show that $\mathbf{1}_{n\equiv a \pmod{q_1}} \approx 1$. Therefore we are going through a two-step approximation process, and exploiting in a crucial manner that $\mathbb{Z}/q_1\mathbb{Z}$ is a subgroup of $\mathbb{Z}/q_1q_2\mathbb{Z}$.

Question 24. When is it helpful to use more complicated intermediate comparison sequences $\mathcal{B}$?

It would be very interesting if we could weaken the requirement that $\mathbb{Z}/q_1q_2\mathbb{Z}$ has a suitably sized subgroup for the arguments to apply.

In various works Drappeau [12, 13] has shown that it can be valuable to retain various possible secondary main terms in applications of Linnik's dispersion method, which corresponds to it being somewhat advantageous to choose a more complicated comparison set $\mathcal{B}$. (A similar feature was used in [62] to help account for Siegel-zero issues.) These can be thought of as examples of intermediate sequences $\mathcal{B}$ which are taking into account the possible causes of fluctuations of the number of primes in $\mathcal{A}$.

10. ABELIAN QUADRATIC LIMITATIONS

One limitation in many methods for counting primes is that we cannot rule out zeros of L-functions very close to the line $\mathrm{Re}(s) = 1$, and so even in the simplest situations such as counting primes in $[1, x]$ we cannot obtain an error term better than some exponential log factor.

One curious feature is that often the more involved counting arguments (such as Type I/II estimates) actually come with much stronger error terms (such as giving a power saving) whenever the estimate can be achieved. For example, the classical exponential sum bound shows that

$$\sum_{n<x} \Lambda(n)e(n\alpha) \ll x^{1-\epsilon}$$

unless $\alpha \approx a/q$ for some $q < x^{2\epsilon}(\log x)^{O(1)}$, in which case the possible existence of a Siegel zero would prevent a power-saving estimate.

Similarly, the error term in the Titchmarsh divisor problem of estimating $\sum_{p<x} \tau(p-1)$ is fundamentally limited by the possible existence of Siegel-zeros (see [13]), but for the analogue of this problem with (normalized) Fourier coefficients of holomorphic cusp forms of $\mathrm{PSL}_2(\mathbb{Z})$, we obtain a power-saving estimate $\sum_{p<x} a(p-1) < x^{391/392+o(1)}$ due to work of Pitt [70].

The 'higher order Fourier analysis' pioneered by Green and Tao [32] involves looking at sums over primes twisted by nilsequences. Again, it is the case that it is ultimately *easier* to obtain quantitative cancellation for nilsequences when the nilsequence is suitably far from a rational phase; the limits of the results stem from possible zeros of Dirichlet L-functions (see, for example, the discussion after [33, THEOREM 1]). Other examples of this occur in the more recent work [55,73] where the ultimately key limitations to estimates are when a nilsequence is 'close' to encoding a rational phase, reducing to the classical situation.

In a slightly different direction, for many situations involving higher degree L-functions it is known that the issue of zeros very close to $s = 1$ cannot arise; Siegel zeros are essentially only a phenomenon which could arise for quadratic Dirichlet L-functions, and so we can have better results in these more complicated scenarios (unless quadratic Dirichlet character could be lurking under the surface, such as if we consider a Dedekind L-function for a number field with an index 2 – so quadratic – subfield).

In all these cases estimates for primes which at first sight seem harder that the classical setting actually avoid the limitations from the well-known obstacles and so prove to actually be easier in some sense.

ACKNOWLEDGMENTS

The author is supported by a Royal Society Wolfson Merit Award, and this project has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement No 851318).

REFERENCES

[1] L. M. Adleman and D. R. Heath-Brown, The first case of Fermat's last theorem. *Invent. Math.* **79** (1985), no. 2, 409–416.

[2] R. C. Baker, G. Harman, and J. Pintz, The difference between consecutive primes. II. *Proc. Lond. Math. Soc. (3)* **83** (2001), no. 3, 532–562.

[3] R. C. Baker and A. J. Irving, Bounded intervals containing many primes. *Math. Z.* **286** (2017), no. 3–4, 821–841.

[4] E. Bombieri, On the large sieve. *Mathematika* **12** (1965), 201–225.

[5] E. Bombieri, J. B. Friedlander, and H. Iwaniec, Primes in arithmetic progressions to large moduli. *Acta Math.* **156** (1986), no. 3–4, 203–251.

[6] E. Bombieri, J. B. Friedlander, and H. Iwaniec, Primes in arithmetic progressions to large moduli. II. *Math. Ann.* **277** (1987), no. 3, 361–393.

[7] E. Bombieri, J. B. Friedlander, and H. Iwaniec, Primes in arithmetic progressions to large moduli. III. *J. Amer. Math. Soc.* **2** (1989), no. 2, 215–224.

[8] J. Bourgain, P. Sarnak, and T. Ziegler, Disjointness of Moebius from horocycle flows. In *From Fourier analysis and number theory to Radon transforms and geometry*, pp. 67–83, Dev. Math. 28, Springer, New York, 2013.

[9] J.-R. Chen, On the representation of a larger even integer as the sum of a prime and the product of at most two primes. *Sci. Sin.* **16** (1973), 157–176.

[10] H. Daboussi and H. Delange, On multiplicative arithmetical functions whose modulus does not exceed one. *J. Lond. Math. Soc. (2)* **26** (1982), no. 2, 245–264.

[11] H. Davenport, *Multiplicative number theory. Second edn*. Grad. Texts in Math. 74, Springer, New York–Berlin, 1980.

[12] S. Drappeau, Théorèmes de type Fouvry–Iwaniec pour les entiers friables. *Compos. Math.* **151** (2015), no. 5, 828–862.

[13] S. Drappeau, Sums of Kloosterman sums in arithmetic progressions, and the error term in the dispersion method. *Proc. Lond. Math. Soc. (3)* **114** (2017), no. 4, 684–732.

[14] S. Drappeau and J. Maynard, Sign changes of Kloosterman sums and exceptional characters. *Proc. Amer. Math. Soc.* **147** (2019), no. 1, 61–75.

[15] N. Elkies, The existence of infinitely many supersingular primes for every elliptic curve over $\mathbb{Q}$. *Invent. Math.* **89** (1987), no. 3, 561–567.

[16] P. D. T. A. Elliott and H. Halberstam, A conjecture in prime number theory. In *Symposia Mathematica, Vol. IV (INDAM, Rome, 1968/69)*, pp. 59–72, Academic Press, London, 1970.

[17] P. Erdős, The difference of consecutive primes. *Duke Math. J.* **6** (1940), 438–441.

[18] K. Ford, Large prime gaps and progressions with few primes. *Riv. Mat. Univ. Parma (N.S.)* **12** (2021), no. 1, 41–47.

[19] K. Ford, B. Green, S. Konyagin, J. Maynard, and T. Tao, Long gaps between primes. *J. Amer. Math. Soc.* **31** (2018), no. 1, 65–105.

[20] K. Ford, B. Green, S. Konyagin, and T. Tao, Large gaps between consecutive prime numbers. *Ann. of Math. (2)* **183** (2016), no. 3, 935–974.

[21] K. Ford and J. Maynard, *An optimal Harman sieve*. In preparation.

[22] E. Fouvry, Autour du théorème de Bombieri–Vinogradov. *Acta Math.* **152** (1984), no. 3–4, 219–244.

[23] E. Fouvry, Théorème de Brun–Titchmarsh: Application au théorème de Fermat. *Invent. Math.* **79** (1985), no. 2, 383–407.

[24] E. Fouvry, E. Kowalski, and P. Michel, On the exponent of distribution of the ternary divisor function. *Mathematika* **61** (2015), no. 1, 121–144.

[25] J. B. Friedlander and H. Iwaniec, Incomplete Kloosterman sums and a divisor problem. *Ann. of Math. (2)* **121** (1985), no. 2, 319–350.

[26] J. B. Friedlander and H. Iwaniec, Asymptotic sieve for primes. *Ann. of Math. (2)* **148** (1998), no. 3, 1041–1065.

[27] J. B. Friedlander and H. Iwaniec, The polynomial $X^2 + Y^4$ captures its primes. *Ann. of Math. (2)* **148** (1998), no. 3, 945–1040.

[28] J. B. Friedlander and H. Iwaniec, *Opera de cribro*. Amer. Math. Soc. Colloq. Publ. 57, American Mathematical Society, Providence, RI, 2010.

[29] D. Goldfeld, The class number of quadratic fields and the conjectures of Birch and Swinnerton-Dyer. *Ann. Sc. Norm. Super. Pisa Cl. Sci. (4)* **3** (1976), no. 4, 624–663.

[30] D. Goldfeld, Gauss's class number problem for imaginary quadratic fields. *Bull. Amer. Math. Soc. (N.S.)* **13** (1985), no. 1, 23–37.

[31] A. Granville, Sieving intervals and Siegel zeros. 2020, arXiv:2010.01211.

[32] B. Green and T. Tao, Linear equations in primes. *Ann. of Math. (2)* **171** (2010), no. 3, 1753–1850.

[33] B. Green and T. Tao, The Möbius function is strongly orthogonal to nilsequences. *Ann. of Math. (2)* **175** (2012), no. 2, 541–566.

[34] B. Gross and D. Zagier, Heegner points and derivatives of L-series. *Invent. Math.* **84** (1986), no. 2, 225–320.

[35] G. Harman, *Prime-detecting sieves*. London Math. Soc. Monogr. Ser. 33, Princeton University Press, Princeton, NJ, 2007.

[36] D. R. Heath-Brown, Prime numbers in short intervals and a generalized Vaughan identity. *Canad. J. Math.* **34** (1982), no. 6, 1365–1377.

[37] D. R. Heath-Brown, The divisor function $d_3(n)$ in arithmetic progressions. *Acta Arith.* **47** (1986), no. 1, 29–56.

[38] D. R. Heath-Brown, Primes represented by $x^3 + 2y^3$. *Acta Math.* **186** (2001), no. 1, 1–84.

[39] D. R. Heath-Brown and H. Iwaniec, On the difference between consecutive primes. *Invent. Math.* **55** (1979), no. 1, 49–69.

[40] D. R. Heath-Brown and C. Jia, The distribution of αp modulo one. *Proc. Lond. Math. Soc. (3)* **84** (2002), no. 1, 79–104.

[41] D. R. Heath-Brown and X. Li, Prime values of $a^2 + p^4$. *Invent. Math.* **208** (2017), no. 2, 441–499.

[42] H. Helfgott, The ternary Goldbach problem. *Ann. of Math. Stud.*. To appear. 2015, arXiv:1501.05438.

[43] C. Hooley, On Artin's conjecture. *J. Reine Angew. Math.* **225** (1967), 209–220.

[44] M. Huxley, On the difference between consecutive primes. *Invent. Math.* **15** (1972), 164–170.

[45] H. Iwaniec, A new form of the error term in the linear sieve. *Acta Arith.* **37** (1980), 307–320.

[46] H. Iwaniec and M. Jutila, Primes in short intervals. *Ark. Mat.* **17** (1979), no. 1, 167–176.

[47] H. Iwaniec and E. Kowalski, *Analytic number theory*. Amer. Math. Soc. Colloq. Publ. 53, American Mathematical Society, Providence, RI, 2004.

[48] C. Jia, On the distribution of αp modulo one. II. *Sci. China Ser. A* **43** (2000), no. 7, 703–721.

[49] I. Kátai, A remark on a theorem of H. Daboussi. *Acta Math. Hungar.* **47** (1986), no. 1–2, 223–225.

[50] X. Li, Prime values of a sparse polynomial sequence. *Duke Math. J.* **171** (2022) no. 1, 101–208.

[51] J. Lichtman, A modification of the linear sieve, and the count of twin primes. 2021, arXiv:2109.02851.

[52] Y. Linnik, *The dispersion method in binary additive problems*. American Mathematical Society, Providence, RI, 1963.

[53] K. Matomäki, The distribution of αp modulo one. *Math. Proc. Cambridge Philos. Soc.* **147** (2009), no. 2, 267–283.

[54] K. Matomäki and M. Radziwiłł, Multiplicative functions in short intervals. *Ann. of Math. (2)* **183** (2016), no. 3, 1015–1056.

[55] K. Matomäki, X. Shao, T. Tao, and J. Teräväinen, Higher uniformity of arithmetic functions in short intervals I. All intervals. 2022, arXiv:2204.03754.

[56] K. Matomäki and J. Teräväinen, On the Möbius function in all short intervals. *J. Eur. Math. Soc.* To appear. 2019, arXiv:1911.09076.

[57] J. Maynard, 3-tuples have at most 7 prime factors infinitely often. *Math. Proc. Cambridge Philos. Soc.* **155** (2013), no. 3, 443–457.

[58] J. Maynard, Small gaps between primes. *Ann. of Math. (2)* **181** (2015), no. 1, 383–413.

[59] J. Maynard, Dense clusters of primes in subsets. *Compos. Math.* **152** (2016), no. 7, 1517–1554.

[60] J. Maynard, Large gaps between primes. *Ann. of Math. (2)* **183** (2016), no. 3, 915–933.

[61] J. Maynard, Primes with restricted digits. *Invent. Math.* **217** (2019), no. 1, 127–218.

[62] J. Maynard, Primes represented by incomplete norm forms. *Forum Math. Pi* **8** (2020), e3, 128.

[63] J. Maynard, Primes in arithmetic progressions to large moduli I: fixed residue classes. *Mem. Amer. Math. Soc.* To appear. 2019, arXiv:2006.06572.

[64] J. Maynard, Primes in arithmetic progressions to large moduli II: well-factorable estimates. *Mem. Amer. Math. Soc.* To appear. 2019, arXiv:2006.07088.

[65] J. Maynard, Primes in arithmetic progressions to large moduli III: uniform residue classes. *Mem. Amer. Math. Soc.* To appear. 2019, arXiv:2006.08250.

[66] J. Maynard and K. Pratt, *Half-isolated zeros and zero density estimates*. 2022, arXiv:2206.11729.

[67] J. Merikoski, The polynomials $X^2 + (Y^2 + 1)^2$ and $X^2 + (Y^3 + Z^3)^2$ also capture their primes. 2021, arXiv:2112.03617.

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

[69] H. L. Montgomery and R. C. Vaughan, The large sieve. *Mathematika* **20** (1973), 119–134.

[70] N. Pitt, On an analogue of Titchmarsh's divisor problem for holomorphic cusp forms. *J. Amer. Math. Soc.* **26** (2013), no. 3, 735–776.

[71] D. H. J. Polymath, Variants of the Selberg sieve, and bounded intervals containing many primes. *Res. Math. Sci.* **1** (2014), Art. 12, 83.

[72] R. A. Rankin, The Difference between Consecutive Prime Numbers. *J. Lond. Math. Soc.* **11** (1936), no. 4, 242–245.

[73] X. Shao and J. Teräväinen, The Bombieri–Vinogradov theorem for nilsequences. *Discrete Anal.* **21** (2021), 55.

[74] T. Tao, The logarithmically averaged Chowla and Elliott conjectures for two-point correlations. *Forum Math. Pi* **4** (2016), e8, 36.

[75] R. Taylor and A. Wiles, Ring-theoretic properties of certain Hecke algebras. *Ann. of Math. (2)* **141** (1995), no. 3, 553–572.

[76] R. C. Vaughan, On the distribution of αp modulo 1. *Mathematika* **24** (1977), no. 2, 135–141.

[77] A. I. Vinogradov, The density hypothesis for Dirichet L-series. *Izv. Ross. Akad. Nauk Ser. Mat.* **29** (1965), 903–934.

[78] I. M. Vinogradov, *The method of trigonometrical sums in the theory of numbers*. Dover Publications, Inc., Mineola, NY, 2004.

[79] N. Watt, Kloosterman sums and a mean value for Dirichlet polynomials. *J. Number Theory* **53** (1995), no. 1, 179–210.

[80] A. Wiles, Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)* **141** (1995), no. 3, 443–551.

[81] S. Y. Xiao, Prime values of $f(a, b^2)$ and $f(a, p^2)$, f quadratic. 2021, arXiv:2111.04136.

[82] Y. Zhang, Bounded gaps between primes. *Ann. of Math. (2)* **179** (2014), no. 3, 1121–1174.

JAMES MAYNARD

Mathematical Institute, Oxford, OX1 4AU, England,
james.alexander.maynard@gmail.com