THREE TOPICS IN ADDITIVE PRIME NUMBER THEORY

BEN GREEN

Abstract. We discuss, in varying degrees of detail, three contemporary themes in prime number theory. Topic 1: the work of Goldston, Pintz and Yıldırım on short gaps between primes. Topic 2: the work of Mauduit and Rivat, establishing that 50% of the primes have odd digit sum in base 2. Topic 3: work of Tao and the author on linear equations in primes.

Introduction. These notes are to accompany two lectures I am scheduled to give at the *Current Developments in Mathematics* conference at Harvard in November 2007. The title of those lectures is 'A good new millennium for primes', but I have chosen a rather drier title for these notes for two reasons. Firstly, the title of the lectures was unashamedly stolen (albeit with permission) from Andrew Granville's entertaining article [16] of the same name. Secondly, and more seriously, I do not wish to claim that the topics chosen here represent a complete survey of developments in prime number theory since 2000 or even a selection of the most important ones. Indeed there are certainly omissions, such as the lack of any discussion of the polynomial-time primality test [2], the failure to even mention the recent work on primes in orbits by Bourgain, Gamburd and Sarnak, and many others.

I propose to discuss the following three topics, in greatly varying degrees of depth. Suggestions for further reading will be provided. The three sections may be read independently although there are links between them.

1. Gaps between primes. Let p_n be the nth prime number, thus $p_1 = 2$, $p_2 = 3$, and so on. The prime number theorem, conjectured by Gauss and proven by Hadamard and de la Vallée Poussin over 110 years ago, tells us that p_n is asymptotic to $n \log n$, or in other words that

$$\lim_{n\to\infty} \frac{p_n}{n \log n} = 1.$$

This implies that the gap between the nth and $(n+1)$st primes, $p_{n+1} - p_n$, is about $\log n$ on average. About 2 years ago Goldston, Pintz and Yıldırım proved the following remarkable result: for any $\epsilon > 0$, there are infinitely many n such that $p_{n+1} - p_n < \epsilon \log n$. That is, infinitely often there are consecutive primes whose spacing is *much* closer than the average.

2. Digits of primes. Written in binary, the first few primes are

$$10, 11, 101, 111, 1011, 1101, 10001, 10011, 10111, \ldots$$

There is no obvious pattern[1]. Indeed, why would there be, since the definition of 'prime' has nothing to do with digital expansions. Proving such a statement, or even formulating it correctly, is an entirely different matter. A couple of years ago, however, Mauduit and Rivat did manage to prove that the digit sum is odd 50% of the time (and hence even 50% of the time). They also obtained results in other bases.

3. Patterns of primes. Additive questions concerning primes have a long history. It has been known for over 70 years that there are infinitely many 3-term arithmetic progressions of primes such as $3, 5, 7$ and $5, 11, 17$, and that every large odd number is the sum of three primes. Recently, in joint work with Tao, we have been able to study more complicated patterns of primes. In this section we provide a guide to this recent joint work.

Throughout these notes we will write

$$\mathbb{E}_{x\in X} f(x) := \frac{1}{X}\sum_{x\in X} f(x),$$

where X is any finite set and $f : X \to \mathbb{C}$ is a function.

1. Gaps between primes

These notes were originally prepared for a series of lectures I gave at the Norwegian Mathematical Society's *Ski og mathematikk*, which took place at Rondablikk in January 2006. It is a pleasure to thank Christian Skau for inviting me to that event. The argument of Goldston, Pintz and Yıldırım was first described to me by K. Soundararajan at the Highbury Vaults in Bristol. It is a pleasure to thank him, and to refer the interested reader to his lectures on the subject [41], which are superior to these in every respect.

1.1. The result.

In 2005 Goldston, Pintz and Yıldırım created a sensation by announcing a proof that

$$\liminf_{n\to\infty} \frac{p_{n+1} - p_n}{\log n} = 0,$$

where p_n denotes the nth prime number. According to the prime number theorem we have

$$p_n \sim n \log n,$$

and therefore

$$\frac{p_{n+1} - p_n}{\log n}$$

has average value 1. The Goldston, Pintz and Yıldırım result thus states that the distance between consecutive primes can be ϵ of the average spacing, for any ϵ, and is thus certainly most spectacular.

[1]Except, of course, that the last digit of primes except the first is always 1.

Previous efforts at locating small gaps between primes focussed on proving successively smaller upper bounds for $C := \liminf_{n\to\infty} \frac{p_{n+1}-p_n}{\log n}$. The following table describing the history of these improvements does not make the Goldston-Pintz-Yıldırım result look any less striking:

		C	
Trivial from PNT		1	
Hardy-Littlewood [27]	1926	2/3	on GRH
Rankin [39]		3/5	on GRH
Erdős [8]	1940	1 - c	unconditionally
Ricci [40]	1954	15/16	
Bombieri-Davenport [4]	1965	0.4665...	
Pilt'ai [38]	1972	0.4571...	
Uchiyama [47]		0.4542...	
Huxley [29, 30, 31]	1984	0.4393...	
Maier [35]	1989	0.2484...	
Goldston-Pintz-Yıldırım	2005	0	

For the detailed proof of this result we refer the reader to the authors' paper [13], as well as to their expository account [12] and to their short article with Motohashi [14]. Our aim here is to give a very rough outline of the proof. One distinctive feature of the argument is that it 'only just' works, in a way that seems rather miraculous. We will endeavour to give some sense of this. We begin with two sections of background material.

1.2. The Elliott-Halberstam Conjecture and level of distribution. Let q be a positive integer and suppose that a is prime to q. We write

$$\psi(N; a, q) := \mathbb{E}_{n\leqslant N, n\equiv a (\mathrm{mod}\, q)}\Lambda(n),$$

where Λ is the von Mangoldt function. For constant q (and in fact for q growing slowly with N, say $q \leqslant (\log N)^A$ for some fixed A) the prime number theorem in arithmetic progressions tells us that

$$\psi(N; a, q) \sim 1/\phi(q).$$

Conditional upon the GRH, we may assert the same result up to about $q \approx N^{1/2}$. The remarkable theorem of Bombieri-Vinogradov (a proof of which the reader will find in many texts on analytic number theory, such as [32]) states that something like this is true *unconditionally*, provided one is prepared to average over q. A weak version of the theorem is that

$$\sum_{q\leqslant Q} \max_{(a,q)=1} |\psi(N; a, q) - \frac{1}{\phi(q)}| \ll_{A,\epsilon} \frac{1}{(\log N)^A} \tag{1.1}$$

for any fixed A and for any $Q \leqslant N^{1/2-\epsilon}$.

By using *sieve theory* one may show that $\psi(N;a,q) \ll N/\phi(q)$, and so the LHS of (1.1) is trivially bounded by

$$\sum_{q \leqslant Q} \frac{1}{\phi(q)} \approx \log Q.$$

The Bombieri-Vinogradov theorem permits us to save an arbitrary power of a logarithm over this trivial bound.

Even conjectures on L-functions (such as the GRH) appear to tell us nothing about the expression (1.1) when $Q \gg N^{1/2}$. Nonetheless, one may make conjectures. If $\theta \in [1/2,1)$ is a parameter then we say that the primes have *level of distribution* θ, or that the *Elliott-Halberstam conjecture* EH(θ) holds, if we have the bound

$$\sum_{q \leqslant Q} \max_{(a,q)=1} |\psi(N;a,q) - \frac{1}{\phi(q)}| \ll_{A,\theta} \frac{1}{(\log N)^A} \tag{1.2}$$

for any $Q \leqslant N^\theta$.

The *full* Elliott-Halberstam conjecture [7] is that EH(θ) holds for all $\theta < 1$. Assuming any Elliott-Halberstam conjecture EH(θ) with $\theta > 1/2$, Goldston, Pintz and Yıldırım can prove the remarkable result that gaps between consecutive primes are infinitely often less than some absolute constant $C(\theta)$. Assuming EH(0.95971), they prove that

$$\liminf_{n\to\infty}(p_{n+1} - p_n) \leqslant 16$$

(actually they prove a slightly weaker result – the value 0.95971 comes from unpublished computations of J. Brian Conrey).

It should be stressed however that it is not expected that any conjecture EH(θ) for $\theta > 1/2$ will be established in the near future. There are results of Bombieri, Friedlander and Iwaniec which go a little beyond the Bombieri-Vinogradov theorem in something resembling the required manner, although experts seem to be of the opinion that these results will not help to improve the bounds on gaps between primes (cf. [1, §16]).

1.3. Selberg's weights. This is the second section of background material.

In the 1940s Selberg introduced a wonderfully simple, yet powerful, idea to analytic number theory. Write 1_P for the characteristic function of the primes. Then if R is any parameter and if $(\lambda_d)_{d\leqslant R}$ is an sequence with $\lambda_1 = 1$, we have the pointwise inequality

$$1_P(n) \leqslant \Big(\sum_{\substack{d|n\\ d\leqslant R}} \lambda_d\Big)^2$$

provided that $n > R$ (the proof is obvious).

This provides an enormous family of majorants for the sequence of primes. In a typical application we will be interested in something like the set of primes p less than some cutoff N, and then R will be some power N^γ, $\gamma < 1$. In this situation Selberg's weights

majorise the primes between N^γ and N, that is to say almost all of the primes less than N.

What weights λ_d should one choose? This depends on the application, but a very basic application is to the estimation of $\frac{1}{y}(\pi(x+y)-\pi(x))$, the density of primes in the interval $(x, x+y]$ (the Brun-Titchmarsh problem). In discussing this problem we will also see why it is advantageous to construct a majorant for the primes, rather than work with 1_P itself.

For any choice of weights λ_d, then, we have

$$\begin{aligned}\frac{1}{y}(\pi(x+y)-\pi(x)) &\leqslant \mathbb{E}_{x+1\leqslant n\leqslant x+y}\Big(\sum_{\substack{d|n\\ d\leqslant R}}\lambda_d\Big)^2\\ &= \sum_{d\leqslant R}\sum_{d'\leqslant R}\lambda_d\lambda_d'\mathbb{E}_{x+1\leqslant n\leqslant x+_y}1_{d|n}1_{d'|n}\\ &= \sum_{d\leqslant R}\sum_{d'\leqslant R}\frac{\lambda_d\lambda_{d'}}{[d,d']}+O\Big(\frac{1}{y}\sum_{d\leqslant R}\sum_{d'\leqslant R}|\lambda_d||\lambda_{d'}|\Big). \qquad (1.3)\end{aligned}$$

Let us imagine that the weights λ_d are chosen to be $\ll y^\epsilon$ in absolute value (this is always the case in practice). Then the second term here is $O(R^2y^{2\epsilon-1})$. If $R\leqslant y^{1/2-2\epsilon}$ then this is $O(y^{-\epsilon})$ and may be thought of as an error term. This is why it is advantageous (indeed essential) to work with a majorant taken over a truncated range of divisors, and not with 1_P itself.

The first term in (1.3),

$$\sum_{d\leqslant R}\sum_{d'\leqslant R}\frac{\lambda_d\lambda_{d'}}{[d,d']},$$

is a quadratic form. It may be explicitly minimised subject to the condition $\lambda_1=1$, giving optimal weights λ_d^{OPT} which are independent of x and y, and the resultant expression may then be evaluated asymptotically. In this way one obtains the well-known bound

$$\frac{1}{y}(\pi(x+y)-\pi(x))\leqslant(2+\epsilon)\frac{\pi(y)}{y},$$

valid for $y>y_0(\epsilon)$.

What is the optimal choice of weights λ_d^{SEL} for the Brun-Titchmarsh problem? The precise form will not concern us here (see, for example, [37]). However, it may be shown that

$$\lambda_d^{\mathrm{SEL}}\approx\mu(d)\frac{\log(R/d)}{\log R}.$$

(For a detailed discussion, see the appendix to [20] and the references to work of Ramaré therein.)

We write

$$\lambda_d^{\mathrm{GY}}:=\mu(d)\frac{\log(R/d)}{\log R}.$$

These weights are very natural for two reasons: their simplicity of form, and the fact that they approximate the optimal weights for the Brun-Titchmarsh problem. There is a third reason for considering them, which comes upon recalling the formula

$$\Lambda(n) = \sum_{d|n} \mu(d) \log(n/d).$$

We see, then, that

$$\Lambda_R(n) := \sum_{\substack{d|n \\ d \leqslant R}} \mu(d) \log(R/d)$$

is a kind of divisor-truncated version of Λ.

We have arrived at the conclusion that the function

$$\frac{1}{(\log R)^2}\Lambda_R^2(n) = \big(\sum_{\substack{d|n \\ d\leqslant R}} \lambda_d^{\mathrm{GY}}\big)^2$$

might be a very useful majorant for the primes.

What might we hope to do with such a majorant? By the computation leading to (1.3), we see that it is possible to find an asymptotic for

$$\mathbb{E}_{N\leqslant n<2N}\Lambda_R(n)^2 \tag{1.4}$$

provided that $R \leqslant N^{1/2-\epsilon}$. Later on we will wish to consider more complicated expressions involving genuine primes, such as

$$\mathbb{E}_{N\leqslant n<2N}\Lambda'(n+2)\Lambda_R(n)^2. \tag{1.5}$$

Here we write Λ' for the von Mangoldt function restricted to primes (as opposed to prime powers), thus

$$\Lambda'(n) := \begin{cases} \log n & \text{if } n \text{ is prime} \\ 0 & \text{otherwise.} \end{cases}$$

The problem of evaluating (1.4) may be thought of as a kind of approximation to the twin prime problem, though we do not know of a way to relate this expression to that problem rigourously. Expanding out, we see that (1.5) is equal to

$$\sum_{d\leqslant R}\sum_{d'\leqslant R} \mu(d)\mu(d')\log(R/d)\log(R/d')\mathbb{E}_{\substack{N\leqslant n<2N \\ [d,d']|n}}\Lambda(n+2).$$

Now we expect that

$$\mathbb{E}_{\substack{N\leqslant n<2N \\ [d,d']|n}}\Lambda'(n+2) \approx \frac{1}{\phi([d,d'])} \tag{1.6}$$

if both d and d' are odd.

The Bombieri-Vinogradov theorem clearly offers a chance of obtaining a statement to this effect *on average* over $d, d' \leqslant R$ if $R \leqslant N^{1/4-\epsilon}$, though there is certainly still work to be done as the distribution of $[d,d']$ as d,d' range over $d,d' \leqslant R$ is not particularly uniform. For the details (which involve moment estimates for divisor functions) see [13, §9].

Once this is done we are left with the main term

$$\sum_{\substack{d\leqslant R\\ d\text{ odd}}}\sum_{\substack{d'\leqslant R\\ d'\text{ odd}}}\frac{\mu(d)\mu(d')}{\phi([d,d'])}\log(R/d)\log(R/d'). \tag{1.7}$$

This term (and related expressions) may all be estimated rather accurately using the standard Dirichlet series techniques of analytic number theory, whereby the sums are expressed as integrals involving products of ζ-functions.

If we had EH(θ), that is to say if the primes had level of distribution θ, one could show that (1.5) is roughly (1.7) in the wider range $R \leqslant N^{\theta/2-\epsilon}$. In particular on the full Elliott-Halberstam conjecture one could work in the range $R \leqslant N^{1/2^{\text{`}}-\epsilon}$, which is essentially the same as for (1.4).

Perhaps we should make a few remarks about the form of the asymptotic for (1.7). One may in fact show that it is

$$\sim \log R \prod_{p\geqslant 3}\big(1-\frac{1}{(p-1)^2}\big).$$

We will see products such as this again in §3.

1.4. A strategy for gaps between primes. We now trun to a discussion of the results of Goldston, Pintz and Yıldırım themselves. From the conceptual viewpoint it is easiest to begin by discussing the very strong *conditional* results proved under the assumption of the Elliott-Halberstam conjecture. We stated in the introduction that they prove

$$\text{liminf}_{n\to\infty}(p_{n+1}-p_n)\leqslant 16 \tag{1.8}$$

assuming EH(θ) for some θ less than 1.

In fact, a much more general result is obtained. Let $\mathcal{H}=\{h_1,\dots,h_k\}$ be a k-tuple of distinct integers with $h_1<h_2<\cdots<h_k$. A generalisation of the twin prime conjecture is that there are infinitely many n such that all of $n+h_1,\dots,n+h_k$ are prime unless this is "obviously impossible for trivial reasons", which would be the case if there is some p such that $\{h_1,\dots,h_k\}$ occupy all residue classes (mod p). If this is *not* the case then we say that $\mathcal{H}$ is *admissible*.

Goldston, Pintz and Yıldırım prove the following.

Theorem 1.4.1. *Suppose that* EH(θ) *is known for some $\theta>1/2$. Then there is $k_0(\theta)$ with the following property. If $k\geqslant k_0(\theta)$ and if $\mathcal{H}=\{h_1,\dots,h_k\}$ is an admissible k-tuple then for infinitely many n at least* two *of the numbers $n+h_1,\dots,n+h_k$ are prime.*

Note in particular that

$$\text{liminf}_{n\to\infty}(p_{n+1}-p_n)\leqslant \min_{\substack{\{h_1,\dots,h_k\}\text{ admissible}\\ k\geqslant k_0(\theta)}}(h_k-h_1).$$

It turns out that $k_0(\theta)$ can be taken to be 6 for $\theta > 0.95971$, and this leads to (1.8) since the 6-tuple $\{0, 4, 6, 10, 12, 16\}$ is admissible.

Here is a very general strategy for detecting primes in admissible tuples. According to [12], this has its origins in work of Selberg and Heath-Brown. Fix a range $[N, 2N)$, suppose that $0 \leqslant h_1 < \cdots < h_k \leqslant N$, and let $(\mu_n)_{N \leqslant n < 2N}$ be arbitrary non-negative weights which are certainly allowed to depend on the h_i. We will compare

$$Q_1 := \mathbb{E}_{N \leqslant n < 2N} \mu_n$$

with

$$Q_2^{(i)} := \frac{1}{\log 3N} \mathbb{E}_{N \leqslant n < 2N} \Lambda'(n + h_i)\mu_n,$$

for $i = 1, \ldots, k$. T. Tao remarked to me that a nice way to think of this as follows: one may renormalise so that $\sum \mu_n = 1$, and then $\rho^{(i)} := Q_2^{(i)}/Q_1$ is essentially the probability that $n + h_i$ is prime if n is drawn at random from the distribution μ (one might then write the expected values in the definitions of Q_1 and $Q_2^{(i)}$ as integrals with respect to μ).

Now if one can choose the weights μ so that $\rho^{(i)} > 1/k$, we will have upon summing over $i = 1, \ldots, k$ that

$$\mathbb{E}_{N \leqslant n < 2N} \big(\sum_{i=1}^{k} \frac{\Lambda'(n + h_i)}{\log 3N} - 1 \big) \mu_n > 0,$$

which means that there is some n such that

$$\Lambda'(n + h_1) + \cdots + \Lambda'(n + h_k) > \log 3N.$$

For such an n, at least two of $n + h_1, \ldots, n + h_k$ are prime. In the probabilistic language, we have essentially used the fact that if $n + h_1, \ldots, n + h_k$ are each drawn at random from μ, the expected number of primes amongst these numbers is > 1.

1.5. Choosing good weights. We continue the discussion of the previous section. How should the weights μ_n be chosen to optimise the factors $\rho^{(i)}$? In retrospect, one may view most of the earlier developments on gaps between primes as attempts to find good weights μ_n in this context – see [13, §4] for further remarks on this.

A very good choice of weights might be

$$\mu_n := \Lambda'(n + h_1) \ldots \Lambda'(n + h_k).$$

One would indeed expect that $\rho^{(i)} \approx 1$ in this case. The only problem is that we have no idea how to prove this, one particular issue being that we cannot show that $Q_1 \neq 0$ (indeed, this is equivalent to finding n such that *all* of $n + h_1, \ldots, n + h_k$ are prime).

We must restrict ourselves to weights μ_n for which it is possible to estimate Q_1 and $Q_2^{(i)}$. As we saw in §1.3, there is a rather large class of such weights. In fact if

$$\mu_n = \big(\sum_{\substack{d | n \\ d \leqslant R}} \lambda_d \big)^2$$

then our chances are good if $R \leqslant N^{\theta/2-\epsilon}$, where θ is the best exponent for which we know EH(θ). Crucially, there is a rather more general class of weights one is able to consider, and that is weights of the form

$$\mu_n = \Big(\sum_{\substack{d|F(n)\\ d\leqslant R}} \lambda_d\Big)^2, \tag{1.9}$$

where $F(n) = (n+a_1)\dots(n+a_m)$ is an integer polynomial. It is an interesting exercise to reprise the arguments of §1.3 in this more general context. In place of the trivial estimate

$$\mathbb{E}_{n\leqslant N, [d,d']|n} 1 = \frac{1}{[d,d']} + O(1)$$

which we used to derive (1.3) one must instead input information about

$$\mathbb{E}_{n\leqslant N, [d,d']|F(n)} 1.$$

But one knows that (for example) $p|F(n)$ precisely if $n \equiv -a_j (\mathrm{mod}\ p)$ for some $j \in \{1,\dots,m\}$, and so such a task is not too frightening. The same is true of sums, such as (1.6), which involve the von Mangoldt function.

For the remainder of the discussion we will narrow down our search for good weights μ_n to those having the form (1.9). We will assume that for any sensible choice of F and the λ_d we may evaluate Q_1 and $Q_2^{(i)}$ for $R \leqslant N^{\theta/2-\epsilon}$ using the standard techniques which we sketched in §1.3.

Now we remarked that an ideal choice of weights is

$$\mu_n = \Lambda'(n+h_1)\dots\Lambda'(n+h_k),$$

but we cannot compute with this choice. A closely related choice of weights is

$$\mu_n = \Lambda_k\big((n+h_1)\dots(n+h_k)\big).$$

Here the function Λ_k is defined by

$$\Lambda_k(n) := \sum_{d|n} \mu(d)\log(n/d)^k,$$

and so in particular $\Lambda_1 = \Lambda$. For general k the function Λ_k is supported on those integers with at most k distinct prime factors. (One way to check this is to use the identity

$$\Lambda_k = L\Lambda_{k-1} + \Lambda * \Lambda_{k-1},$$

where $L(n) := \log n$ and $*$ denotes Dirichlet convolution.)

Now in §1.3 we saw the advantages of replacing Λ with Λ_R, a divisor-truncated version of it. By analogy one might consider

$$\Lambda_{k,R}(n) := \sum_{\substack{d|n\\ d\leqslant R}} \mu(d)\log(R/d)^k.$$

This could be negative, but its square $\Lambda_{k,R}^2$ certainly cannot. Furthermore

$$\mu_n := \Lambda_{k,R}^2((n+h_1)\dots(n+h_k))$$

is of the form (1.9) (with $F(n) = (n+h_1)\dots(n+h_k)$). This, then, is a very natural choice of the weights μ_n and it is with some anticipation that we await the results of computing Q_1 and the $Q_2^{(i)}$, and hence the factors $\rho^{(i)}$. What we obtain is this:

$$\rho^{(i)} \sim \frac{2}{k+1} \cdot \frac{\log R}{\log N}.$$

This is something of a disappointment, since it is not greater than $1/k$ even when $R = N^{\theta/2-\epsilon}$ for θ very close to 1 (that is, with a very strong form of the Elliott-Halberstam conjecture).

Astonishingly, a seemingly small change tips the balance in our favour. We consider instead

$$\mu_n := \Lambda^2_{k+l,R}((n+h_1)\dots(n+h_k)),$$

where $0 < l \ll k$ is a further parameter. In the probabilistic language, $\rho^{(i)}$ may then be thought of (very roughly) as something like the probability that $n+h_i$ is prime given that $(n+h_1)\dots(n+h_k)$ has at most $k+l$ prime factors.

With this choice of weights it is possible to compute that

$$\rho^{(i)} \sim \frac{2k}{k+2l+1}\frac{2l+1}{l+1} \cdot \frac{\log R}{\log N}. \tag{1.10}$$

Note that as $k, l \to \infty$ with $l = o(k)$, this is essentially $4\log R/k\log N$. In particular with $R := N^{\theta/2-\epsilon}$ one has $\rho^{(i)} > 1/k$ for $k \geqslant k_0(\theta)$, for any $\theta > 1/2$. This is enough to establish Theorem 1.4.1.

1.6. The unconditional result. In this section we explain some aspects of the proof that

$$\liminf_{n\to\infty} \frac{p_{n+1}-p_n}{\log n} = 0.$$

Recall that in the last section we chose weights

$$\mu_n := \Lambda^2_{k+l,R}((n+h_1)\dots(n+h_k)).$$

Taking $R := N^{1/4-\epsilon}$, the quantities Q_1 and $Q_2^{(i)}$ can be evaluated using the Bombieri-Vinogradov theorem (rather than the Elliott-Halberstam conjecture). If k, l are large with $l \ll k$ then (from (1.10)) the quantities $\rho^{(i)}$ are all at least $1/k - \epsilon'$ for $k \geqslant k_1(\epsilon)$, and hence we have that

$$\mathbb{E}_{N\leqslant n<2N}\Big(\sum_{i=1}^{k} \frac{\Lambda'(n+h_i)}{\log 3N}\Big)\mu_n \geqslant (1-\delta)\|\mu\|_1, \tag{1.11}$$

for any $\delta > 0$, and any $k \geqslant k_2(\delta)$. Here

$$\|\mu\|_1 := \mathbb{E}_{N\leqslant n<2N}\mu_n$$

is the total mass of μ. This means that if n is drawn at random from the distribution μ, then the expected number of primes amongst the numbers $n+h_1, \dots n+h_k$ is at least $1-\delta$. Clearly, this is not an immediately applicable result if one wishes to obtain two or more primes in the tuple $\{n+h_1, \dots, n+h_k\}$.

There is, however, a tiny bit of further information available to us. Even if $h_0 \notin \{h_1, \dots, h_k\}$, there is still a chance that if n is drawn at random from μ then $n+h_0$ will be prime. One can work out that this probability is asymptotically

$$\frac{\mathfrak{S}(h_0, h_1, \dots, h_k)}{\log N},$$

where $\mathfrak{S}(h_0, h_1, \dots, h_k)$ is a certain *singular series* reflecting the arithmetic properties of the numbers $h_0, h_1, \dots, h_k$ (it is similar in form to the product defining the twin prime constant). Formally what we mean by this is that

$$\mathbb{E}_{N \leqslant n < 2N} \frac{\Lambda'(n+h_0)}{\log 3N} \mu_n \sim \frac{\mathfrak{S}(h_0, h_1, \dots, h_k)}{\log N} \|\mu\|_1,$$

and this may once again be rigorously established using the Bombieri-Vinogradov theorem.

Let $\eta > 0$ be arbitrary. Summing over all h_0 with

$$0 \leqslant h_0 \leqslant \eta \log N,$$

we obtain from (1.11) that

$$\mathbb{E}_{N \leqslant n < 2N} \Big(\sum_{h=0}^{\eta \log N} \frac{\Lambda'(n+h)}{\log 3N} \Big) \mu_n \geqslant \left(1 - \delta + \sum_{\substack{h_0 = 0 \\ h_0 \notin \{h_1, \dots, h_k\}}}^{\eta \log N} \frac{\mathfrak{S}(h_0, h_1, \dots, h_k)}{\log N} \right) \|\mu\|_1. \quad (1.12)$$

For a typical choice of $h_1, \dots, h_k$, the right-hand side will be of a predictable size. Indeed by a result of Gallagher one may infer that

$$\sum_{\substack{h_0, \dots, h_k \leqslant H \\ h_i \text{ distinct}}} \mathfrak{S}(h_0, h_1, \dots, h_k) \sim H^{k+1}$$

as $H \to \infty$. Taking expectations over all k-tuples $\{h_1, \dots, h_k\}$ of distinct integers with $0 \leqslant h_i \leqslant \eta \log N$, we therefore obtain from (1.12) that

$$\mathbb{E}_{N \leqslant n \leqslant 2N} \Big(\sum_{h=0}^{\eta \log N} \frac{\Lambda'(n+h)}{\log 3N} \Big) \mu_n \geqslant (1 - \delta + \eta - o(1)) \|\mu\|_1.$$

Recall that this is valid for any $\delta > 0$, provided that k is sufficiently large. Taking $\delta = \eta/2$, we therefore see that (if n is drawn at random from μ) the expected number of primes in the interval $[n, n + \eta \log N]$ is strictly greater than 1. In particular there is some such interval containing at least two primes.

1.7. Further results. Since the original paper of Goldston, Pintz and Yıldırım several further works have appeared or are scheduled to appear giving refinements and variants of the main theorem. Here is a summary of what has been done:

- In the forthcoming paper [10] it is shown, by refining the ideas just described as far as seems possible, that

$$\liminf_{n \to \infty} \frac{p_{n+1} - p_n}{(\log p_n)^{1/2} (\log \log p_n)^2} < \infty.$$

This remarkable result asserts that the gap between primes is infinitely often almost as small as the *square root* of the average gap.

- Let $q_1 < q_2 < \dots$ be the numbers which are the product of exactly two distinct primes. Then
$$\liminf_{n\to\infty}(q_{n+1} - q_n) \leqslant 26,$$
and in fact
$$\liminf_{n\to\infty}(q_{n+1} - q_n) \leqslant 6$$
if one assumes the Elliott-Halberstam conjecture. These results are obtained in the paper [11] by the three authors and S. W. Graham.
- In the original paper [13] one also finds results concerning several primes bunching together. Thus assuming EH(θ) one has, for any $r \geqslant 2$, the bound
$$\liminf_{n\to\infty} \frac{p_{n+r} - p_n}{\log p_n} \leqslant (\sqrt{r} - \sqrt{2\theta})^2.$$
One rather curious feature of this bound is that the full Elliott-Halberstam conjecture EH(1) implies that
$$\liminf_{n\to\infty} \frac{p_{n+2} - p_n}{\log p_n} = 0.$$
Nothing of this sort is known for $p_{n+3} - p_n$, even conditionally.

2. Binary digits of primes

These notes originated from a course I lectured in Part III of the Mathematical Tripos at Cambridge University in the Lent Term 2007. My aim was to work through the result of Mauduit and Rivat in the case of binary expansions of primes, and to produce a reasonably short exposition (the original paper is 49 pages long). Because we provide complete details this section is considerably more technical than either §1 or §3. Readers not interested in these technicalities may still wish to read §2.3.

2.1. Statement of results.

In a recent preprint [36], Mauduit and Rivat proved that asymptotically 50% of the primes have odd digit sum in base 2 (and hence, of course, 50% of the primes have *even* digit sum in base 2 as well!), answering a long-standing question of Gelfond. Our aim in this section is to give a self-contained proof of their theorem in the following form, which is easily seen to imply the result as just stated.

Theorem 2.1.1 (Mauduit-Rivat)**.** *Let Λ be the von-Mangoldt function, and let $s : \mathbb{N} \to \mathbb{N}$ be the function which sums the binary digits of n. Then*
$$\mathbb{E}_{n\leqslant X}\Lambda(n)(-1)^{s(n)} = O(X^{-\delta})$$
for some $\delta > 0$.

In fact Mauduit and Rivat proved rather more than this: they counted primes whose digit sum in base q is congruent to $a (\mathrm{mod}\ m)$, for any natural numbers a, q, m. To prove

a result in this generality requires some extra technical devices and a lot more notation, so we leave the interested reader to consult the original paper [36].

I find the result intrinsically interesting, but another reason for studying it is that it represents a pleasingly self-contained example of Vinogradov's method of 'Type I and II sums' or 'bilinear forms' for handling prime number sums.

In contrast with the last chapter we provide a fairly complete technical discussion.

2.2. Some notation. Throughout this section X will be thought of as a large parameter. If Y_1 and Y_2 are two quantities which depend on X we write $Y_1 \gtrapprox Y_2$ if $Y_1 \gg_\epsilon X^{-\epsilon}Y_2$ for all $\epsilon > 0$. We use the notation $Y_1 \lessapprox Y_2$ similarly. Typically we might have $Y_1 \gg Y_2 \log^{-C} X$ for some C, but the notation is occasionally applied in even looser situations. For example we have the bound $\tau(x) \lessapprox 1$ uniformly in $x \leqslant X$, where $\tau(x)$ denotes the number of divisors of x.

If $n \in \mathbb{N}$ we write $\nu_2(n)$ for the 2-exponent of n, the maximal r such that $2^r|n$.

The letter c will always denote a small, positive, absolute constant. Different instances of the letter will not necessarily denote the same constant.

2.3. Vinogradov's method of Type I/II sums. Suppose that $f : \mathbb{N} \to \mathbb{C}$ is a function, bounded by 1. This section concerns a method which can be often be used to show that a sum of the form

$$\mathbb{E}_{n \leqslant X} \Lambda(n) f(n)$$

is substantially smaller than X. The method is particularly inclined to work when f is "far" from being multiplicative. It is clear that such a sum *cannot* be small in many cases when f does have some multiplicative tendancies, for example when $f(n) = \mu(n)$ or when $f(n)$ is a Dirichlet character to small modulus.

We will develop a develop a form of the method which includes some technical refinements particularly suited to the study of the function $f(n) = (-1)^{s(n)}$. These are rather insubstantial and consist in large part of ensuring that various cutoffs are exact powers of two. In these notes we will endow the $\sim$ symbol with a rather specific meaning: if we write $\sum_{n \sim 2^\nu}$ then we understand that the variable n is to range over the dyadic interval $[2^{\nu-1}, 2^\nu)$.

Here is the version of Vinogradov's method that we shall require.

Proposition 2.3.1 (Method of Type I/II sums)**.** *Suppose that $f : \mathbb{N} \to \mathbb{C}$ is a function with $|f(n)| \leqslant 1$ for all n. Let $\delta \in (0, 1]$ be a parameter. We say that* Type I sums are δ-small *if*

$$\frac{1}{X} \sum_{m \sim 2^\mu} |\sum_{n \in I_m} f(mn)| \leqslant \delta$$

whenever $2^\mu \leqslant X^{1/100}$, $I_m \subseteq [2^{\nu-1}, 2^\nu)$ *is an interval and* $2^{\mu+\nu} \leqslant X$. *We say that* Type II sums are δ-small *if*

$$\frac{1}{X}\Big|\sum_{m\sim 2^\mu}\sum_{n\sim 2^\nu} a_m b_n f(mn)\Big| \leqslant \delta$$

uniformly for all sequences $(a_m), (b_n)$ *with* $|a_m|, |b_n| \leqslant 1$ *and for all* μ, ν *such that* $X^{1/100} \leqslant 2^\mu, 2^\nu \leqslant X^{99/100}$. *Suppose that* f *is a function for which Type I and Type II sums are* δ*-small. Then*

$$\mathbb{E}_{n\leqslant X}\Lambda(n)f(n) \ll \delta^{1/2}\log^C X.$$

Remarks. One can take $C = 11/2$. Note that both Type I and Type II sums are trivially bounded by X. The important feature of the proposition, then, is that a big enough gain over these trivial bounds leads to an improvement of the trivial bound on $\mathbb{E}_{n\leqslant X}\Lambda(n)f(n)$, which is $O(\log X)$.

In our statement of the result we have made a particular choice of the the ranges of μ, ν for which estimates for Type I/II sums are required. There is considerable flexibility in the choice of these ranges. Though this matter does not concern us here, we remark that it has apparently not been completely clarified in the literature (though see [6, §8] for a related discussion).

When is an attempt to use the method of Type I/II sums likely to be successful in establishing a non-trivial bound for $\mathbb{E}_{n\leqslant X}\Lambda(n)f(n)$? In general, one might hope for success when f does not behave "multiplicatively". Certainly if f is multiplicative, say $f = \chi$ for some Dirichlet character χ, then by choosing $a_m = \overline{f(m)}$ and $b_n = \overline{f(n)}$ we see that the Type II sums are *not* always small. A similar phenomenon persists for those f which are the sum of a few multiplicative functions, for example the additive character $f(n) = e(an/q)$ with q a small integer. Fortunately one can estimate $\mathbb{E}_{n\leqslant X}\Lambda(n)f(n)$ for these functions by other means, namely the explicit formula and theorems on the location of zeroes of L-functions.

If, on the other hand, f does not exhibit significant multiplicative behaviour then one may hope that the method of Type I and II sums will work. The most classical instance of this, worked out by Vinogradov in the course of proving that every large odd number is the sum of three primes, is the case $f(n) = e(\alpha n)$ where α is not close to a rational a/q. Our task here is to handle the case $f(n) = (-1)^{s(n)}$.

2.4. Proof of the method of Type I/II sums. Even though Proposition 2.3.1 is not normally stated with quite the same technical refinements that we have done, the reader familiar with the basics of this theory may prefer to skip this somewhat technical section.

Before making a start on the proof proper, we show that the assumption that Type II sums are small implies that Type I sums are small for a much larger range of μ than we have hypothesised.

Lemma 2.4.1 (Type II implies extended Type I)**.** *Suppose that $f : \{1, \dots, N\} \to \mathbb{C}$ is a function with $\|f\|_\infty \leqslant 1$ for which Type I and Type II sums are δ-small. Then we have the Type I estimate*

$$\frac{1}{X} \sum_{m \sim 2^\mu} \Big| \sum_{n \in I_m} f(mn) \Big| \ll \delta \log X$$

in range $2^\mu \leqslant X^{99/100}$.

Proof. Since Type I sums are δ-small, we may assume that $2^\mu \geqslant X^{1/100}$. It clearly suffices to prove that

$$\frac{1}{X} \sum_{m \sim 2^\mu} \sum_{n \sim 2^\nu} \omega_m 1_{I_m}(n) f(mn) \ll \delta \log X \tag{2.1}$$

for all choices of ω_m with $|\omega_m| = 1$. But for the cutoff $1_{I_m}(n)$, which does not factor as a product of a function of m with a function of n, this looks like a Type II sum. To remove the cutoff, we employ a standard "separation of variables" trick. By the Fourier inversion formula on $\mathbb{Z}$ we have

$$1_{I_m}(n) = \int_0^1 \widehat{1}_{I_m}(\theta) e(n\theta)\, d\theta.$$

Thus the left-hand side of (2.1) is equal to

$$\frac{1}{X} \int_0^1 \Big(\sum_{m \sim 2^\mu} \sum_{n \sim 2^\nu} \omega_m \widehat{1}_{I_m}(\theta) e(\theta n) f(mn) \Big)\, d\theta.$$

Since Type II sums are δ-small and

$$|\widehat{1}_{I_m}(\theta)| \ll \min(X, |\theta|^{-1})$$

we see that this is at most

$$\delta \int_0^1 \min(X, |\theta|^{-1})\, d\theta \ll \delta \log X.$$

This concludes the proof. □

Proof of Proposition 2.3.1. The argument is essentially that of Vaughan [48], but I have followed the beautiful presentation in the book of Iwaniec and Kowalski [32]. We start with the easily-verified relation

$$\Lambda(n) = \sum_{\substack{b,c \\ bc|n}} \Lambda(b)\mu(c).$$

Let $U := X^{1/3}$ (say), and decompose this sum as

$$\Lambda(n) = \Lambda_{\sharp\sharp}(n) + \Lambda_{\sharp\flat}(n) + \Lambda_{\flat\sharp}(n) + \Lambda_{\flat\flat}(n),$$

where $\flat$ denotes "large" divisors and $\sharp$ denotes "small" divisors, so that for example

$$\Lambda_{\flat\sharp}(n) := \sum_{\substack{b \geqslant U, c < U \\ bc|n}} \Lambda(b)\mu(c).$$

We observe that

$$\Lambda_{\sharp\flat}(n) + \Lambda_{\sharp\sharp}(n) = \sum_{b<U} \Lambda(b) \sum_{c|\frac{n}{b}} \mu(c) = 1_{n<U}$$

whilst

$$\begin{aligned}\Lambda_{\flat\sharp}(n) + \Lambda_{\sharp\sharp}(n) &= \sum_{\substack{c<U\\ c|n}} \mu(c) \sum_{b|\frac{n}{c}} \Lambda(b)\\ &= \sum_{\substack{c<U\\ c|n}} \mu(c)\log(n/c).\end{aligned}$$

Thus we obtain what is essentially *Vaughan's identity*,

$$\Lambda(n) = -\Lambda_{\sharp\sharp}(n) + \Lambda_{\flat\flat}(n) + 1_{n<U}\Lambda(n) + \sum_{\substack{c<U\\ c|n}} \mu(c)\log(n/c). \tag{2.2}$$

Weighting by $f(n)$ and summing over $n \leqslant X$ we obtain

$$\begin{aligned}&\sum_{n\leqslant X} \Lambda(n)f(n)\\ &= -\sum_{n\leqslant X} \Lambda_{\sharp\sharp}(n)f(n) + \sum_{n\leqslant X} \Lambda_{\flat\flat}(n)f(n) + \sum_{n<U} \Lambda(n)f(n) + \sum_{\substack{c<U\\ c|n}} \mu(c) \sum_{n\leqslant X} f(n)\log(n/c)\\ &= S_1 + S_2 + S_3 + S_4.\end{aligned}$$

Our objective is to use the assumption that Type I and II sums are small in order to bound the sums S_i.

Bounding S_1. We have

$$S_1 = \sum_{b,c<U} \Lambda(b)\mu(c) \sum_{n\leqslant X/bc} f(bcn).$$

This may be rewritten as

$$\sum_{m<U^2} \omega_m \sum_{n\leqslant X/m} f(mn), \tag{2.3}$$

where

$$\omega_m := \sum_{\substack{b,c<U\\ bc=m}} \Lambda(b)\mu(c).$$

By splitting into $O(\log^2 X)$ dyadic ranges for m and n, we see that it suffices to prove that

$$\sum_{m\sim 2^\mu} |\omega_m| \Big| \sum_{n\in I_m} f(mn)\Big| \ll \delta^{1/2} X \log^{C-2} X \tag{2.4}$$

whenever $I_m \subseteq [2^{\nu-1}, 2^\nu)$ is an interval and $2^{\mu+\nu} \leqslant X$. This does not quite follow from Lemma 2.4.1 since ω_m is not bounded. We do, however have $|\omega_m| \ll \tau(m)\log X$, where τ is the divisor function, and hence since $\sum_{n\leqslant N} \tau(n)^2 \ll N\log^3 N$ we have

$$\sum_{m\sim 2^\nu} |\omega_m|^2 \ll 2^\mu \log^5 X.$$

This means that for any $Q > 0$ we have the estimate

$$\sum_{\substack{m\sim 2^\mu \\ |\omega_m|>Q}} |\omega_m| \ll 2^\mu Q^{-1} \log^5 X.$$

Splitting the sum in (2.4) into two parts according as $|\omega_m|$ is or is not greater that Q we obtain

$$\sum_{m\sim 2^\mu} |\omega_m| \Big| \sum_{n\in I_m} f(mn)\Big| \ll Q^{-1} X \log^5 X + Q \sum_{m\sim 2^\mu} \Big| \sum_{n\in I_m} f(mn)\Big|.$$

By Lemma 2.4.1 this is bounded by

$$Q^{-1} X \log^6 X + \delta Q X \log X.$$

Choosing $Q := \delta^{-1/2} \log^{5/2} X$, we obtain a bound of the required type.

Bounding S_2. The sum S_2 may be written as

$$\sum_{b,c\geqslant U} \sum_{t\leqslant X/bc} \Lambda(b)\mu(c) f(bct).$$

Changing variables and rearranging, this may be written as

$$\sum_{\substack{m\geqslant U \\ mn\leqslant X}} a_m b_n f(mn), \tag{2.5}$$

where $a_m := \Lambda(m)$ and $b_n := \sum_{c\geqslant U : c|n} \mu(c)$. Observing that $b_n = 0$ if $n < U$, we see that the sum over m, n is covered by $O(\log^2 X)$ dyadic ranges $m \sim 2^\mu$, $n \sim 2^\nu$ with $X^{0.01} \leqslant 2^\mu, 2^\nu \leqslant X^{0.99}$. We may therefore split (2.5) into $O(\log^2 X)$ sums of the form

$$\sum_{m\sim 2^\mu} \sum_{n\sim 2^\nu} 1_{I(n)}(m) a_m b_n f(mn), \tag{2.6}$$

where $I(n) \subseteq [2^{\mu-1}, 2^\mu)$ is an interval. It suffices to show that any such sum is $\ll \delta^{1/2} X \log^{C-2} X$.

These sums look rather like Type II sums, except for the presence of the cutoff $1_{I(n)}(m)$ and the fact that the sequences a_m, b_n are not bounded.

To remove the cutoff we use the same device as in the proof of Lemma 2.4.1, writing (2.6) as

$$\int_0^1 \Big(\sum_{m\sim 2^\mu} \sum_{n\sim 2^\nu} a_m e(\theta m) \widehat{1}_{I(n)}(\theta) b_n f(mn)\Big)\, d\theta.$$

Since $|\widehat{1}_{I(n)}(\theta)| \ll \min(X, |\theta|^{-1})$ we see that it suffices to prove that

$$\sum_{m\sim 2^\mu} \sum_{n\sim 2^\nu} a'_m b'_n f(mn) \ll \delta^{1/2} X \log^{C-3} X$$

uniformly for all choices of a'_m with $|a'_m| \leqslant |a_m|$ and $|b'_n| \leqslant |b_n|$ for all m, n.

This has effectively removed the cutoff that we were worried about. It remains to deal with the non-boundedness of the sequences $(a'_m)_{m\sim 2^\mu}, (b'_n)_{n\sim 2^\nu}$. The non-boundedness

of a'_m is rather minor, since clearly $a'_m \leqslant \log X$ for all m. Thus we may define $a''_m := a'_m/\log X$ and reduce to proving that

$$\sum_{m\sim 2^\mu}\sum_{n\sim 2^\nu} a''_m b'_n f(mn) \ll \delta^{1/2} X \log^{C-4} X \tag{2.7}$$

whenever $|a''_m| \leqslant 1$. To deal with b'_n, we note that $|b'_n| \leqslant \tau(n)$. Thus, by the argument used in dealing with S_1, we have

$$\sum_{\substack{n\sim 2^\nu \\ |b'_n|\geqslant Q}} |b'_n| \ll 2^\nu Q^{-1} \log^3 X.$$

Splitting the sum in (2.7) into parts according as $|b'_n| \geqslant Q$ or not, we conclude as before.

Bounding S_3. The sum S_3 is trivially bounded by $U = X^{1/3}\log X$. The δ-smallness of Type I sums implies (rather vacuously) that $|f(n)| \leqslant \delta X$. Since we are assuming that $\|f\|_\infty = 1$, it follows that $\delta \geqslant 1/X$ and hence this term may be absorbed into the bound $\delta^{1/2} X \log^C X$ that we are trying to establish.

Bounding S_4. The sum may be written as

$$\sum_{m\leqslant U}\sum_{n\leqslant X/m} \mu(m)\log n f(mn).$$

This may be split into $O(\log^2 X)$ sums of the form

$$\sum_{m\sim 2^\mu}\sum_{n\in I_m} \mu(m)\log n f(mn), \tag{2.8}$$

where $I_m \subseteq [2^{\nu-1}, 2^\nu)$. This is almost a Type I sum: only the presence of the $\log n$ term prevents it being so. This term is so smooth, however, that it may be effectively removed by "partial summation". To do this, simply write

$$\log n = \int_1^n \frac{dt}{t}$$

and rearrange (2.8) as

$$\int_1^{2^\nu} \frac{dt}{t} \sum_{m\sim 2^\nu} \mu(m) \sum_{n\in I_{m,t}} f(mn),$$

where $I_{m,t} \subseteq [2^{\nu-1}, 2^\nu)$ is an interval. The smallness of Type I sums, as given in Lemma 2.4.1, may now be used to see that this is bounded as required.

This completes the bounding of S_4, and hence the proof of Proposition 2.3.1. □

2.5. The sum-of-digits function and related functions. If n is a positive integer and $n = \sum_{i\geqslant 0} n_i 2^i$ is its binary expansion, we write

$$s(n) := \sum_i n_i.$$

This is, of course, a finite sum. For each positive integer k we consider also the truncated functions

$$s_k(n) := \sum_{i=0}^{k-1} n_i.$$

These functions are closely related to $s(n)$, of course; on any interval $[2^k t, 2^k(t+1))$ the functions $s_k(n)$ and $s(n)$ differ by a fixed constant. The truncated functions $s_k(n)$ are periodic with period 2^k, however, and this makes them rather amenable to study using Fourier analysis on the finite group $\mathbb{Z}/2^k\mathbb{Z}$.

In fact we will be more interested in the oscillatory functions

$$f(n) := (-1)^{s(n)}$$

and

$$f_k(n) := (-1)^{s_k(n)}.$$

The functions s_k and f_k may, by abuse of notation, be regarded as functions on $\mathbb{Z}/2^k\mathbb{Z}$.

Definition 2.5.1 (Finite Fourier transform)**.** Let $k \geqslant 0$ be a fixed integer. Then we define

$$\widehat{f_k}(r) := \mathbb{E}_{x \in \mathbb{Z}/2^k\mathbb{Z}} f_k(x) e(-rx/2^k).$$

We now proceed to establish several properties of the Fourier transform $\widehat{f_k}$ which will be useful later on. We collect these here since they are all proved in a very similar way. The reader might wish to read through the proof of the first one, then skip to the next section. She might return here as each result is required.

Proposition 2.5.2 (L^∞ bound)**.** *We have* $|\widehat{f_k}(r)| \ll 2^{-ck}$ *for all* $r \in \mathbb{Z}/2^k\mathbb{Z}$.

Proof. We observe that

$$\widehat{f_k}(r) = 2^{-k}(1 - e(t))(1 - e(2t)) \dots (1 - e(2^{k-1}t)), \tag{2.9}$$

where $t = r/2^k$. The result now follows by observing that

$$|1 - e(u)||1 - e(2u)| = 4|\sin(\pi u)\sin(2\pi u)| = 8|\cos(\pi u)|(1 - \cos^2(\pi u))$$

is maximised when $\cos^2(\pi u) = 1/3$, and attains the value $16/3\sqrt{3}$ there. Thus, grouping terms in pairs, we see that

$$\widehat{f_k}(r) \ll (4/3\sqrt{3})^{k/2} \ll 2^{-k/10}.$$

This concludes the proof. □

Proposition 2.5.3 (L^1 bound in progressions)**.** *Suppose that* $0 \leqslant k' \leqslant k$ *and that* a *is a residue class* $(\mathrm{mod}\, 2^{k'})$*. Then*

$$\sum_{\substack{r \in \mathbb{Z}/2^k\mathbb{Z} \\ r \equiv a (\mathrm{mod}\, 2^{k'})}} |\widehat{f_k}(r)| \ll 2^{(\frac{1}{2}-c)(k-k')} |\widehat{f_{k'}}(a)|.$$

Remark. For the purposes of discussion suppose that $k' = a = 0$. Then this proposition states that

$$\sum_{r \in \mathbb{Z}/2^k\mathbb{Z}} |\widehat{f_k}(r)| \ll 2^{(\frac{1}{2}-c)k}.$$

By contrast the trivial bound (arising from Parseval's identity and an application of Cauchy-Schwarz) for this quantity would be $2^{k/2}$.

One tends to imagine that a saving over a trivial bound can be expected whenever there is some kind of "cancellation", such as one might expect if the function $f_k : \mathbb{Z}/2^k\mathbb{Z} \to \{-1, 1\}$ were chosen at random. This setting is rather different, and this represents perhaps the most remarkable feature of the paper [36]. It is possible to show that if f_k is chosen randomly then

$$\sum_{r \in \mathbb{Z}/2^k\mathbb{Z}} |\widehat{f_k}(r)| \gg 2^{k/2}.$$

Our proposition therefore captures a very specific property of the functions $f_k(n) = (-1)^{s_k(n)}$.

Proof. Write $S(a, k)$ for the sum on the left. For any $r \in \mathbb{Z}/2^k\mathbb{Z}$ the expansion (2.9) yields

$$|\widehat{f_k}(r)| = \tfrac{1}{2}|1 - e(r/2^k)||\widehat{f_{k-1}}(r)|.$$

Suppose that $k \geqslant k' + 1$. Since $\widehat{f_{k-1}}(r)$ is periodic with period 2^{k-1}, we may split $S(a, r)$ as a sum over two ranges $0 \leqslant r < 2^{k-1}$ and $2^{k-1} \leqslant r < 2^k$, thereby obtaining

$$S(a, k) \leqslant S(a, k-1) \sup_{t \in [0,1]} \tfrac{1}{2}\big(|1 + e(t)| + |1 - e(t)|\big).$$

Now a simple exercise in Euclidean geometry confirms that

$$|1 + e(t)| + |1 - e(t)| \leqslant 2\sqrt{2}, \tag{2.10}$$

with equality if and only if $t = \pm 1/4$. Hence

$$S(a, k) \leqslant \sqrt{2}S(a, k-1). \tag{2.11}$$

This does not, in itself, suffice to establish a nontrivial bound for $S(a, k)$.

If $k \geqslant k' + 2$ one may improve things by splitting the sum $S(a, k)$ into *four* ranges $j2^{k-2} \leqslant r < (j + 1)2^{k-2}$ $(j = 0, 1, 2, 3)$. This leads to

$$S(a, k) \leqslant S(a, k-2) \sup_{t \in [0,1]} \tfrac{1}{4} \sum_{j=0}^{3} |1 - e(t + j/4)||1 - e(2(t + j/4))|. \tag{2.12}$$

Now two applications of (2.10) confirm that

$$\begin{aligned}
&\sum_{j=0}^{3} |1 - e(t + j/4)||1 - e(2(t + j/4))| \\
&\quad = |1 - e(2t)|\big(|1 - e(t)| + |1 + e(t)|\big) + |1 + e(2t)|\big(|1 - e(t + 1/4)| + |1 + e(t + 1/4)|\big) \\
&\quad \leqslant 2\sqrt{2}\big(|1 - e(2t)| + |1 + e(2t)|\big) \\
&\quad \leqslant 8.
\end{aligned}$$

Furthermore equality can never occur, and so by compactness this expression is bounded by $8-c$ for some $c>0$. Comparing with (2.12) we see that

$$S(a,k) \leqslant (2-c)S(a,k-2).$$

To complete the proof of the proposition one may apply this repeatedly, followed perhaps by one application of (2.11), to bound $S(a,k)$ above in terms of $S(a,k')$. □

2.6. Analysis of Type I sums.

Proposition 2.6.1 (Estimate for Type I sums)**.** *Suppose that $2^\mu \leqslant X^{1/20}$. For each $m \sim 2^\mu$, suppose that $I_m \subseteq (2^{\nu-1}, 2^\nu]$ is an interval. Then*

$$\sum_{m\sim 2^\mu} |\sum_{n\in I_m} f(mn)| \ll_\epsilon X^{19/20+\epsilon}.$$

Remark. In [36] an alternative argument (related to the large sieve) is used, in which the same estimate is established under the weaker assumption that $2^\mu = O_\epsilon(X^{1/2-\epsilon})$. *Proof.* For m,n in the ranges under consideration we have have $f(mn) = f_k(mn)$, where $k := \mu+\nu$. Fix a value of m, and write $S_m := \sum_{n\in I_m} f(mn)$. We thus have

$$S_m = \sum_{x\in\mathbb{Z}/2^k\mathbb{Z}} f(x)1_P(x),$$

where $P = P_m := \{mn : n \in I_m\}$. By Parseval's identity this is

$$2^k \sum_{r\in\mathbb{Z}/2^k\mathbb{Z}} \widehat{f_k}(r)\widehat{1}_P(r),$$

which is bounded by $2^k\|\widehat{f_k}\|_\infty\|\widehat{1}_P\|_1$. By summing a geometric series we have

$$|\widehat{1}_P(r)| \ll \min(1, \|r/2^k\|^{-1}),$$

and therefore $\|\widehat{1}_P\|_1 \ll k \ll \log X$. It follows from Lemma 2.5.2 that

$$S_m \ll 2^k X^{-1/10}\log X.$$

Summing over $m\sim 2^\mu$, we obtain the required bound. □

2.7. Two diophantine lemmas.

In this section we give two results of a 'diophantine' nature which we will use in the next section, in which Type II sums are analysed. Both of these are more-or-less standard in this subject.

Lemma 2.7.1 (Vinogradov)**.** *Suppose that q,Q,R are all natural numbers less than X, that $\beta\in\mathbb{R}$, and suppose that $(a,q)=1$. Then*

$$\sum_{x=0}^{R} \min\left(Q, \|ax/q+\beta\|^{-1}\right) \lessapprox Q+q+R+QR/q.$$

Proof. The key observation is that as x ranges over any interval of length q, the numbers $ax/q (\mathrm{mod}\ 1)$ range over the set $0, 1/q, \dots, (q-1)/q$. It follows easily that if I is any interval of length at most q then

$$\sum_{x \in I} \min\left(Q, \|ax/q + \beta\|^{-1}\right) \ll Q + q \log q.$$

Since the range $x = 1, \dots, R$ may be split into at most $R/Q + 1$ such ranges, the result follows immediately. □

Lemma 2.7.2 (Equidistribution lemma)**.** *Suppose that $\alpha \in \mathbb{R}$ and that I is an interval of integers with $|I| = N$. Suppose that δ_1, δ_2 satisfy $\delta_1 < \delta_2/16$, and suppose that there are at least $\delta_2 N$ elements $n \in I$ for which $\|\alpha n\|_{\mathbb{R}/\mathbb{Z}} \leqslant \delta_1$. Suppose that $N \geqslant 8/\delta_2$. Then there is some $q \leqslant 8/\delta_2$ such that $\|\alpha q\|_{\mathbb{R}/\mathbb{Z}} \leqslant 4\delta_1\delta_2^{-1}N^{-1}$.*

Proof. By a well-known argument of Dirichlet there is some $q \leqslant N$ and an a coprime to q such that $|\alpha - a/q| \leqslant 1/qN$. Set $\theta := \alpha - a/q$, let $n_0 \in I$ be fixed, and set $\beta := n_0\theta$. Then for any $n \in I$ we have, by the triangle inequality,

$$\|\alpha n\|_{\mathbb{R}/\mathbb{Z}} \geqslant \|an/q + \beta\|_{\mathbb{R}/\mathbb{Z}} - \|\theta(n - n_0)\|_{\mathbb{R}/\mathbb{Z}} \geqslant \|an/q + \beta\|_{\mathbb{R}/\mathbb{Z}} - 1/q,$$

and so

$$\|an/q + \beta\|_{\mathbb{R}/\mathbb{Z}} \leqslant \delta_1 + \frac{1}{q} \tag{2.13}$$

for at least $\delta_2 N$ values of $n \in I$.

Now as n ranges over any interval of length q the numbers an/q range over the set $\{0, 1/q, 2/q, \dots\}$. Thus in any such interval the number of n satisfying (2.14) is no more than $\delta_1 q + 2$. Now I may be divided into at most $N/q + 1$ intervals of length no more than q, and thus the number of $n \in I$ satisfying (2.13) is bounded by

$$(\frac{N}{q} + 1)(\delta_1 q + 2).$$

On the other hand, we are assuming this quantity is at least $\delta_2 N$. Since $\delta_2 \geqslant 4\delta_1$, $N \geqslant 8/\delta_2$ and $q \leqslant N$ this easily implies that $q \leqslant 8/\delta_2$.

Now the assumption of the lemma implies, by piegonholing, that $\|\alpha n\|_{\mathbb{R}/\mathbb{Z}} \leqslant 2\delta_1$ for at least $\delta_2 N/2$ values of $n \in \{1, \dots, N/2\}$. We have

$$\alpha n = \frac{an}{q} + \theta n$$

where $|\theta| \leqslant 1/qN$. If $n \leqslant N/2$, it follows that either

$$\|\alpha n\|_{\mathbb{R}/\mathbb{Z}} \geqslant 1/2q \geqslant \delta_2/16 > \delta_1$$

or else n is a multiple of q. But for $k \leqslant N/2q$ we have simply

$$\|\alpha kq\|_{\mathbb{R}/\mathbb{Z}} = |\theta kq|.$$

Thus $|\theta kq| \leqslant 2\delta_1$ for at least $\delta_2 N/2$ such values of k, and in particular for some $k_0 \geqslant \delta_2 N/2$. Hence $|\theta| \leqslant 2\delta_1/qk_0 \leqslant 4\delta_1/q\delta_2 N$, which implies the result. □

2.8. Analysis of Type II sums. We start with an inequality which is often used in the estimation of Type II sums, van der Corput's inequality.

Van der Corput's inequality. Van der Corput's inequality is a kind of generalisation of the Cauchy-Schwarz inequality.

Lemma 2.8.1 (van der Corput inequality)**.** *Let N, H be positive integers and suppose that $(a_n)_{n\in\{1,\dots,N\}}$ is a sequence of complex numbers. Extend (a_n) to all of $\mathbb{Z}$ by defining $a_n := 0$ when $n \notin \{1,\dots,N\}$. Then*

$$|\sum_n a_n|^2 \leqslant \frac{N+H}{H}\sum_{|h|\leqslant H}\big(1-\frac{|h|}{H}\big)\sum_n a_n\overline{a_{n+h}}.$$

Proof. We have

$$\sum_n a_n = \frac{1}{H}\sum_{-H<n\leqslant N}\sum_{h=0}^{H-1} a_{n+h}.$$

Thus, applying the Cauchy-Schwarz inequality, we have

$$\begin{aligned}|\sum_n a_n\big|^2 &= \frac{1}{H^2}\big|\sum_{-H<n\leqslant N}\sum_{h=0}^{H-1} a_{n+h}\big|^2\\ &\leqslant \frac{N+H}{H^2}\sum_{-H<n\leqslant N}\big|\sum_{h=0}^{H-1} a_{n+h}\big|^2\\ &= \frac{N+H}{H^2}\sum_{-H<n\leqslant N}\sum_{h=0}^{H-1}\sum_{h'=0}^{H-1} a_{n+h}\overline{a}_{n+h},\end{aligned}$$

which equals the right hand side of the claimed inequality. This concludes the proof. □

Proposition 2.8.2 (Estimate for Type II sums)**.** *Suppose that $X^{1/100} \leqslant 2^\mu, 2^\nu \leqslant X^{99/100}$. Suppose that $(a_m)_{m\sim 2^\mu}$ and $(b_n)_{n\sim 2^\nu}$ are arbitrary sequences of complex numbers with $|a_m|, |b_n| \leqslant 1$. Then*

$$\sum_{m\sim 2^\mu}\sum_{n\sim 2^\nu} a_m b_n f(mn) \ll X^{1-\kappa}$$

for some absolute $\kappa > 0$.

Proof. We may assume without loss of generality that $\nu \geqslant \mu$. Suppose for a contradiction that the result is false. We write this

$$\sum_{m\sim 2^\mu}\sum_{n\sim 2^\nu} a_m b_n f(mn) \gtrapprox 2^{\mu+\nu}.$$

By Cauchy-Schwarz we obtain

$$\sum_{m\sim 2^\mu}|\sum_{n\sim 2^\nu} b_n f(mn)|^2 \gtrapprox 2^{\mu+2\nu}.$$

Let $\rho := c(\mu+\nu)$, where $c > 0$ is a constant to be chosen later, and apply the van der Corput inequality (Lemma 2.8.1) with $H := 2^\rho$. It follows that

$$\sum_{m\sim 2^\mu}\sum_{n\sim 2^\nu}\sum_{|h|\leqslant H}\big(1-\frac{|h|}{H}\big)b_n\overline{b_{n+h}}f(m(n+h))f(mn) \gtrapprox 2^{\mu+\nu+\rho}.$$

The $h=0$ term is negligible, and so we obtain

$$\sum_{1\leqslant|h|\leqslant 2^\rho}\sum_{n\sim 2^\nu}|\sum_{m\sim 2^\mu}f(m(n+h))f(mn)| \gtrapprox 2^{\mu+\nu+\rho}. \tag{2.14}$$

Our aim is to obtain some cancellation in the inner sum and thereby reach a contradiction. The first step is to show that f can be replaced by the truncated function f_k, where $k := \mu + 2\rho$ (say) is not much bigger than μ.

Now we have

$$s(m(n+h)) - s_k(m(n+h)) = s(mn) - s_k(mn)$$

if $mn, m(n+h)$ lie in the same interval $[2^k t, 2^k(t+1)]$. Since mh is much smaller than 2^k, this will happen most of the time. In fact for it not to hold we must have $mn \in [2^k t - 2^{\mu+\rho}, 2^k t]$ for some t (that is, there is a "carry" on adding mh to mn). Now for $x \leqslant X$ the divisor function τ satisfies $\tau(x) \lessapprox 1$, and therefore the number of "bad" pairs (m,n) is at most

$$\sum_{t\leqslant 2^{\nu-2\rho}}\sum_{l=2^k t-2^{\mu+\rho}}^{2^k t}\tau(l) \lessapprox 2^{\mu+\nu-\rho}.$$

The contribution of the bad pairs to (2.14) is therefore negligible, and we may replace that inequality by

$$\sum_{1\leqslant|h|\leqslant 2^\rho}\sum_{n\sim 2^\nu}|\sum_{m\sim 2^\mu}f_k(m(n+h))\overline{f_k(mn)}| \gtrapprox 2^{\mu+\nu+\rho}. \tag{2.15}$$

Let us now focus on the inner sum

$$E_{n,h} := \sum_{m\sim 2^\mu} f_k(m(n+h))f_k(mn),$$

which we will study using Fourier analysis on $\mathbb{Z}/2^k\mathbb{Z}$. Expanding both copies of f_k using the inversion formula, we see that

$$E_{n,h} = \sum_{m\sim 2^\mu}\sum_{r,s\in\mathbb{Z}/2^k\mathbb{Z}}\widehat{f_k}(r)\widehat{f_k}(s)e\big(\frac{rm(n+h)+smn}{2^k}\big),$$

which is bounded by

$$\sum_{r,s\in\mathbb{Z}/2^k\mathbb{Z}}|\widehat{f_k}(r)||\widehat{f_k}(s)|\min(2^\mu, \|\frac{r(n+h)+sn}{2^k}\|^{-1}).$$

From (2.15) we thus have

$$\sum_{r,s\in\mathbb{Z}/2^k\mathbb{Z}}|\widehat{f_k}(r)||\widehat{f_k}(s)|\sum_{n\sim 2^\nu}\sum_{1\leqslant|h|\leqslant 2^\rho}\min(2^\mu, \|\frac{r(n+h)+sn}{2^k}\|^{-1}) \gtrapprox 2^{\mu+\nu+\rho}. \tag{2.16}$$

Define the weights

$$\omega_{r,s} := 2^{-\mu-\nu-\rho}\sum_{n\sim 2^\nu}\sum_{1\leqslant|h|\leqslant 2^\rho}\min(2^\mu, \|\frac{r(n+h)+sn}{2^k}\|^{-1}).$$

Then (2.16) becomes

$$\sum_{r,s\in\mathbb{Z}/2^k\mathbb{Z}}|\widehat{f_k}(r)||\widehat{f_k}(s)|\omega_{r,s}\gtrapprox 1. \tag{2.17}$$

To do anything with this we need to gain a greater understanding of the weights $\omega_{r,s}$.

Lemma 2.8.3 (Size of $\omega_{r,s}$)**.** *Suppose that $\nu_2(r+s)=t$. Then*

$$\omega_{r,s}\lessapprox 2^{-\mu}+2^{k-t-\mu-\nu}+2^{t-k}.$$

Proof. Write $(r+s)/2^k = a/2^{k-t}$, where is odd. Thus

$$\omega_{r,s} = 2^{-\mu-\nu-\rho}\sum_{n\sim 2^\nu}\sum_{1\leqslant|h|\leqslant 2^\rho}\min\big(2^\mu, \|\frac{a}{2^{k-t}}n+\frac{r}{2^k}h\|^{-1}\big).$$

Thus

$$\omega_{r,s}\leqslant 2^{-\mu-\nu}\sup_{1\leqslant|h|\leqslant 2^\rho}\sum_{n\sim 2^\nu}\min(2^\mu, \|\frac{a}{2^{k-t}}n+\frac{r}{2^k}h\|^{-1})$$

By Lemma 2.7.1 we obtain

$$\omega_{r,s}\lessapprox 2^{-\nu}+2^{-\mu}+2^{k-t-\mu-\nu}+2^{t-k}.$$

Recalling that $\nu\geqslant\mu$, we see that this implies the claimed bound. □

Let us recall (2.17). This clearly implies that there is t, $0\leqslant t\leqslant k$, such that

$$\sum_{\substack{r,s\in\mathbb{Z}/2^k\mathbb{Z}\\ \nu_2(r+s)=t}}|\widehat{f_k}(r)||\widehat{f_k}(s)|\omega_{r,s}\gtrapprox 1. \tag{2.18}$$

Now by Lemma 2.8.3, Proposition 2.5.3 and Parseval's inequality (in turn) we have

$$\begin{aligned}
&\sum_{\substack{r,s\in\mathbb{Z}/2^k\mathbb{Z}\\ \nu_2(r+s)=t}}|\widehat{f_k}(r)||\widehat{f_k}(s)|\omega_{r,s}\\
&\lessapprox (2^{-\mu}+2^{k-t-\mu-\nu}+2^{t-k})\sum_{a\in\mathbb{Z}/2^t\mathbb{Z}}\sum_{r\equiv a(\mathrm{mod}\,2^t)}|\widehat{f_k}(r)|\sum_{s\equiv -a(\mathrm{mod}\,2^t)}|\widehat{f_k}(s)|\\
&\lessapprox 2^{(k-t)(1-c)}(2^{-\mu}+2^{k-t-\mu-\nu}+2^{t-k})\sum_{a\in\mathbb{Z}/2^t\mathbb{Z}}|\widehat{f_t}(a)||\widehat{f_t}(-a)|\\
&\leqslant 2^{(k-t)(1-c)}(2^{-\mu}+2^{k-t-\mu-\nu}+2^{t-k})
\end{aligned}$$

for some absolute constant $c>0$. Recalling that $k=\mu+2\rho$ we see that the first two terms are at most $2^{4\rho-ck}$, which is not $\gtrapprox 1$ if ρ is chosen sufficiently small. Thus we see that if (2.18) holds then $2^{-c(k-t)}\gtrapprox 1$, which implies that $2^t\gtrapprox 2^k$.

Assume, then, that this is the case. Applying Parseval's identity again (or Proposition 2.5.3, but this is overkill now) we obtain, for any ε,

$$\sum_{\substack{r,s\in\mathbb{Z}/2^k\mathbb{Z}\\ \nu_2(r+s)=t\\ \omega_{r,s}\leqslant 2^{-\varepsilon k}}} |\widehat{f_k}(r)||\widehat{f_k}(s)|\omega_{r,s} \leqslant 2^{-\varepsilon k} \sum_{a\in\mathbb{Z}/2^t\mathbb{Z}} \sum_{r\equiv a (\mathrm{mod}\, 2^t)} |\widehat{f_k}(r)| \sum_{s\equiv -a (\mathrm{mod}\, 2^t)} |\widehat{f_k}(s)|$$

$$\leqslant 2^{k-t-\varepsilon k} \lessapprox 2^{-\varepsilon k}.$$

It follows that, in (2.18), we may restrict attention to values of r, s for which $\omega_{r,s} \gtrapprox 1$, thus

$$\sum_{\substack{r,s\in\mathbb{Z}/2^k\mathbb{Z}\\ \omega_{r,s}\gtrapprox 1}} |\widehat{f_k}(r)||\widehat{f_k}(s)|\omega_{r,s} \gtrapprox 1. \tag{2.19}$$

In the next lemma we will show that there are rather few pairs (r, s) with $\omega_{r,s} \gtrapprox 1$. To do this we will make use of the as yet unexploited averaging over h which occurs in the definition of $\omega_{r,s}$.

Lemma 2.8.4 (Large values of $\omega_{r,s}$)**.** *There are $\lessapprox 2^\rho$ pairs $(r, s) \in \mathbb{Z}/2^k\mathbb{Z} \times \mathbb{Z}/2^k\mathbb{Z}$ such that $\omega_{r,s} \gtrapprox 1$.*

Proof. We know already, by Lemma 2.8.3, that we must have $\nu_2(r + s) = t$, where $2^t \gtrapprox 2^k$. Write $(r + s)/2^k = a/2^{k-t}$, where a is odd. We have

$$\sum_{1\leqslant |h|\leqslant 2^\rho} \sum_{n\sim 2^\nu} \min(2^\mu, \|\frac{a}{2^{k-t}}n + \frac{r}{2^k}h\|^{-1}) \gtrapprox 2^{\mu+\nu+\rho}.$$

Dividing the sum over n into residue classes (mod 2^{k-t}), of which there are $\lessapprox 1$, we see that there is θ such that

$$\sum_{1\leqslant |h|\leqslant 2^\rho} \min(2^\mu, \|\theta + \frac{r}{2^k}h\|^{-1}) \gtrapprox 2^{\mu+\rho}. \tag{2.20}$$

Although this looks to be of the form covered by Vinogradov's lemma (Lemma 2.7.1), the fact that $2^\rho \lll 2^k$ means that more information may be gleaned by appealing instead to Lemma 2.7.2. From (2.20) it follows that for $\gtrapprox 2^\rho$ values of h, $1 \leqslant |h| < 2^\rho$, we have

$$\|\theta + \frac{r}{2^k}h\| \lessapprox 2^{-\mu}.$$

Fixing some h_0 with this property and considering the numbers $h - h_0$, we may assume that $\theta = 0$. Applying Lemma 2.7.2, we see that

$$\|qr/2^k\|_{\mathbb{R}/\mathbb{Z}} \lessapprox 2^{-\mu-\rho}$$

for some $q \lessapprox 1$. Thus if $\omega_{r,s} \gtrapprox 1$ then there is some $q \lessapprox 1$ such that $|rq (\mathrm{mod}\, 2^k)| \lessapprox 2^\rho$ (recall that $k = \mu + 2\rho$). There are $\lessapprox 2^\rho$ such values of r, and for each of them there are just $\lessapprox 1$ values of s such that $t := \nu_2(r + s)$ satisfies $2^t \gtrapprox 2^k$. □

It is now an easy matter to show that (2.19) cannot hold which, as we have shown, implies that Type II sums are small. Indeed using Lemma (2.8.4) and Proposition 2.5.2 we obtain

$$\sum_{\substack{r,s\in\mathbb{Z}/2^k\mathbb{Z}\\ \omega_{r,s}\gtrapprox 1}} |\widehat{f_k}(r)||\widehat{f_k}(s)|\omega_{r,s} \lessapprox 2^{\rho-2ck}.$$

This contradicts (2.19) if ρ is chosen sufficiently small. □

Proof of Theorem 2.1.1. Almost nothing more need be said: Theorem 2.1.1 is an immediate consequence of Propositions 2.3.1, 2.6.1 and 2.8.2. □

3. Patterns of primes

The aim of this section is to discuss work of the author and T. Tao on linear equations in primes. This programme is not yet completed and what has been done so far is spread across a number of papers [21, 22, 23, 24, 25, 26]. It is also discussed in several expository articles [17, 19, 42, 43, 44].

Our aim here is to do little more than try to describe what we have proved and what we hope to prove, and to furnish the reader with some idea of how the various papers fit together. In other words we hope that this section may be used as a sort of 'roadmap' for readers interested in a more detailed study of the papers. There are some conspicuous absences from the current section. Our treatment of the history of the subject is very patchy (see the article [34] for this), and we omit any discussion of links with the ergodic theory literature (see [28, 33] for this). References are to the versions of the papers which were available on `www.arxiv.org` on October 1st 2007. It is quite likely that published versions will have different theorem numberings.

Suppose that $\psi_1, \dots, \psi_t : \mathbb{Z}^d \to \mathbb{Z}$ are affine-linear forms. The basic questions which motivate our work are the following.

Question 3.0.5 (Existence of prime values)**.** Are there values of $\vec{n} \in \mathbb{Z}^d$ for which these forms all take prime values? Are there infinitely many such $\vec{n}$?

Question 3.0.6 (Asymptotics)**.** How many such $\vec{n}$ are there inside the box $[-N, N]^d$?

In this generality, our questions contain many of the classical questions in additive prime number theory.

(i) When $d = 1$, $t = 2$, $\psi_1(n) = n$ and $\psi_2(n) = 2m - n$ we have the *Goldbach Conjecture*: is $2m$ the sum of two primes?
(ii) When $d = 1$, $t = 2$, $\psi_1(n) = n$ and $\psi_2(n) = n + 2$ we have the *Twin Prime Conjecture*: are there infinitely pairs of primes which differ by 2?

(iii) When $d = 2$, $t = 3$, $\psi_1(\vec{n}) = n_1$, $\psi_2(\vec{n}) = n_2$ and $\psi_3(\vec{n}) = m - n_1 - n_2$ (m odd) we have the *Ternary Goldbach Conjecture*: is m the sum of three primes?
(iv) When $d = 2$, $t = k$ and $\psi_i(\vec{n}) = n_1 + (i-1)n_2$, $i = 1, \dots, k$ we have the question of whether there exist arithmetic progressions of length k consisting entirely of primes.

Essentially nothing is known about either Question 3.0.5 or Question 3.0.6 in cases (i) and (ii). Both Questions were answered in case (iii) some seventy years ago by Vinogradov, building on earlier work of Hardy and Littlewood. Question 3.0.5 was answered in case (iv) by the author and Tao [21]. Question 3.0.6 in that case is much harder and was answered for $k = 3$ by Chowla and van der Corput in 1939 and for $k = 4$ by the author and Tao [22, 23, 24]. Question 3.0.6 for $k \geqslant 5$ is one of the main goals of our current programme of research, and we shall report on what progress has been made so far. We will not give any further separate discussion of Question 3.0.5, as this has now been exposited in many places. Particularly recommended are the articles [28] and [33]. See also [19, 42, 43, 44].

There are very natural conjectural answers to Questions 3.0.5 and 3.0.6. It is clear that congruence conditions may result in there being no, or very few, choices of $\vec{n}$ for which all of the forms $\psi_i(\vec{n})$ are prime. A trivial example is the system $\psi_1(n) = n, \psi_2(n) = n + 7$ – consideration of this (mod 2) obviously implies that $\psi_1(n)$ and $\psi_2(n)$ cannot both be prime. Congruence conditions may alter our expectations in more subtle ways too. For example if n is known to be prime (and is not 2) then one feels that $n+2$ is *more* likely to be prime than a random integer of the same size, for it is already known to be odd. Pulling against this, however, is the observation that if $n \neq 3$ then n is congruent to either 1 or 2(mod 3), and so $n + 2$ is congruent to either 0 or 1(mod 3), but never to 2. On this (mod 3) evidence one feels that $n + 2$ is *less* likely to be prime than a random integer of the same size. Another obvious way in which one could fail to have any prime values among the $\psi_i(\vec{n})$ is if they cannot be simultaneously positive, for example $\psi_1(\vec{n}) = n_1 - n_2$, $\psi_2(\vec{n}) = n_2 - n_3$, $\psi_3(\vec{n}) = n_3 - n_1$.

A more profound analysis of these intuitions suggests the following conjecture. In the formulation of this conjecture we use the *local* von Mangoldt functions $\Lambda_{\mathbb{Z}/p\mathbb{Z}}$, defined by

$$\Lambda_{\mathbb{Z}/p\mathbb{Z}}(x) = \begin{cases} p/(p-1) & \text{if } (x,p) = 1 \\ 0 & \text{otherwise.} \end{cases}$$

Dickson's Conjecture. *Suppose that $d, t, N \geqslant 1$ are integers. Suppose that no two of the forms ψ_i are rational multiples of one another, and that no form ψ_i is constant. Write $\psi_i(\vec{n}) = l_{i1}n_1 + \cdots + l_{id}n_d + b_i$ and suppose that we have $|l_{ij}| \leqslant L$, $|b_i| \leqslant LN$ for some real number L. Then for any convex body $K \subseteq [-N, N]^d$ we have*

$$\sum_{\vec{n} \in K \cap \mathbb{Z}^d} \Lambda(\psi_1(\vec{n})) \dots \Lambda(\psi_d(\vec{n})) = \beta_\infty \prod_p \beta_p + o_{d,t,L}(N^d),$$

where the local factors β_p are defined by

$$\beta_p := \mathbb{E}_{\vec{x} \in (\mathbb{Z}/p\mathbb{Z})^d} \Lambda_{\mathbb{Z}/p\mathbb{Z}}(\psi_1(\vec{x})) \dots \Lambda_{\mathbb{Z}/p\mathbb{Z}}(\psi_d(\vec{x}))$$

and

$$\beta_\infty := \mathrm{vol}(K \cap \psi_1^{-1}(\mathbb{R}_{\geqslant 0}) \cap \cdots \cap \psi_t^{-1}(\mathbb{R}_{\geqslant 0})).$$

Remarks. We have counted primes weighted using the von Mangoldt function, as this gives tidier expressions. For an unweighted version see [24, Conjecture 1.4]. It is quite fun to play with particular cases of the conjecture. For example with $d = 1$, $t = 2$, $\psi_1(n) = n$, $\psi_2(n) = n + 2$ and $K = [0, N]$ we obtain the conjecture

$$\sum_{n \leqslant N} \Lambda(n)\Lambda(n+2) = 2\prod_{p \geqslant 3} \big(1 - \frac{1}{(p-1)^2}\big)N + o(N)$$

for the (weighted) number of twin primes less than or equal to N. The numerical value of the constant here is about 1.32. Some other examples are worked out in [24, §1].

Let us return to the specific examples (i) – (iv) mentioned above. What makes some of these questions much easier than others? The most important parameter in determining the difficulty of Questions 3.0.5 and 3.0.6 is the *complexity* of the system of forms $\{\psi_1, \dots, \psi_t\}$.

The definition of complexity involves nothing more than simple linear algebra, but it is not especially illuminating at first sight. Let s be a positive integer. We say that the complexity of the system $\{\psi_1, \dots, \psi_t\}$ is at most s if, for any $i \in \{1, \dots, t\}$, the forms $\{\psi_1, \dots, \psi_{i-1}, \psi_{i+1}, \dots, \psi_t\}$ may be divided into $s+1$ classes in such a way that ψ_i is not in the affine linear span of any of them. Thus the system $\{n_1, n_1+n_2, n_1+2n_2, n_1+3n_2\}$ has complexity at most 2 since, quite obviously, we may remove any one form and divide the remaining three forms into singleton classes whose affine span does not contain that form. However the complexity of this system is *not* at most 1: if we remove the form n_1 then it is impossible to divide the remaining forms $\{n_1+n_2, n_1+2n_2, n_1+3n_2\}$ into two classes such that n_1 is not in the affine linear span of any class. Thus the complexity of this system is exactly two. The complexity of the system $\{n_1, n_1 + n_2, n_1 + 2n_2\}$ is one, as is the complexity of the system $\{n_1, n_2, m - n_1 - n_2\}$ for any fixed m. The complexity of the system $\{n, n+2\}$ is apparently undefined, since if we remove the form n it is impossible to partition the singleton class $\{n + 2\}$ in any way such that n is not contained in the affine span of a class. In such cases we say that the complexity is infinite. The system $\{n, 2m - n\}$, m fixed, arising from the Goldbach Conjecture has infinite complexity.

Roughly speaking, only systems of complexity one were understood before the recent work [22, 23, 24]. Much of the theory in the complexity one case was worked out in a paper of Balog [3], which built upon the techniques of Vinogradov.

Complexity is the most important measure of how difficult it is to solve Questions 3.0.5 and 3.0.6. However there are some rather trivial examples of systems of complexity greater than one for which Question 3.0.5 can be answered. For example just using the fact that there are $\gg N/\log N$ primes less than N and the Cauchy-Schwarz inequality it is possible to show that there are $\gg N^4/\log^8 N$ quadruples (n_1, n_2, n_3, n_4) such that

all eight of the forms

$$\{n_1, n_1+n_2, n_1+n_3, n_1+n_4, n_1+n_2+n_3, n_1+n_2+n_4, n_1+n_3+n_4, n_1+n_2+n_3+n_4\}$$

are prime. This system has complexity 2.

The reason that complexity one systems have proved amenable to attack is that they can be studied using *harmonic analysis*, and in particular the circle method of Hardy and Littlewood. We are now going to discuss some ideas behind this method in a rather unorthodox way. It turns out that this is the easiest (in fact so far the only) description to generalize to systems of complexity 2 and higher. The following formulation of the principle that 'harmonic analysis governs systems of complexity 1' is established in [24].

Proposition 3.0.7. *Let N be a prime. Suppose that $\{\psi_1, \dots, \psi_t\}$ is a system of affine-linear forms of complexity 1. Suppose that $f_1, \dots, f_t : \mathbb{Z}/N\mathbb{Z} \to [-1,1]$ are functions and that*

$$|\mathbb{E}_{\vec{n} \in (\mathbb{Z}/N\mathbb{Z})^d} f_1(\psi_1(\vec{n})) \dots f_t(\psi_t(\vec{n}))| \geqslant \delta. \tag{3.1}$$

Then for each $i \in [t]$ there is some $r \in \mathbb{Z}/N\mathbb{Z}$ such that

$$|\mathbb{E}_{n \in \mathbb{Z}/N\mathbb{Z}} f_i(n) e(-rn/N)| \gg_\delta 1. \tag{3.2}$$

In words, if the functions $f_1, \dots, f_t$ behave in some way unexpectedly when evaluated along the linear forms ψ_i, this phenomenon can be detected by evaluating the Fourier coefficients of the f_i.

Proposition 3.0.7 is proved in two stages. The first step is to establish a *generalized von Neumann theorem*, which is a bound of the form

$$|\mathbb{E}_{\vec{n} \in (\mathbb{Z}/N\mathbb{Z})^d} f_1(\psi_1(\vec{n})) \dots f_t(\psi_t(\vec{n}))| \leqslant \inf_{i \in [t]} \|f_i\|_{U^2}.$$

Here $\|f\|_{U^2}$ denotes the *Gowers U^2-norm* of f and is defined by

$$\|f\|_{U^2}^4 := \mathbb{E}_{x,h_1,h_2 \in \mathbb{Z}/N\mathbb{Z}} f(x)\overline{f(x+h_1)f(x+h_2)}f(x+h_1+h_2).$$

Results of this type are proved using nothing more than a few applications of the Cauchy-Schwarz inequality, although the notation can get quite complicated. A simple example is given in the proof of [18, Proposition 1.9]. Foundational material on the Gowers norms (including, for example, a proof that they *are* norms) may be found in [46, Chapter 11] or [21, Chapter 5].

This first step in the proof of Proposition 3.0.7 leads from the hypothesis (3.1) to the conclusion that each $\|f_i\|_{U^2}$ is at least δ. To obtain the conclusion (3.2), then, it suffices to establish an *Inverse Theorem* for the Gowers U^2-norm, stating that if the U^2-norm of f is large then f correlates with a linear phase.

The proof of this result is so short we give it here. Suppose that $f : \mathbb{Z}/N\mathbb{Z} \to [-1,1]$ is a function with $\|f\|_{U^2} \geqslant \delta$. Define the Fourier transform $\hat{f} : \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}$ by

$$\hat{f}(r) := \mathbb{E}_{n \in \mathbb{Z}/N\mathbb{Z}} f(n) e(-rn/N).$$

Using orthogonality relations one may easily check that

$$\|\hat{f}\|_4 := \big(\sum_{r\in\mathbb{Z}/N\mathbb{Z}} |\hat{f}(r)|^4\big)^{1/4} = \|f\|_{U^2}. \tag{3.3}$$

Thus

$$\|\hat{f}\|_\infty^2 \|\hat{f}\|_2^2 \geqslant \|\hat{f}\|_4^4 \geqslant \delta^4.$$

But by Parseval's identity we have

$$\|\hat{f}\|_2 = \|f\|_2 \leqslant 1,$$

and so we conclude that

$$\|\hat{f}\|_\infty \geqslant \delta^2.$$

That is, there is some $r \in \mathbb{Z}/N\mathbb{Z}$ such that

$$|\mathbb{E}_{n\in\mathbb{Z}/N\mathbb{Z}} f(n)e(-rn/N)| \geqslant \delta^2. \tag{3.4}$$

We note that (3.3) also gives a converse result: *if* there is some $r \in \mathbb{Z}/N\mathbb{Z}$ such that

$$|\mathbb{E}_{n\in\mathbb{Z}/N\mathbb{Z}} f(n)e(-rn/N)| \geqslant \delta$$

then $\|f\|_{U^2} \geqslant \delta$.

Proposition 3.0.7 is a somewhat convincing way to formulate the idea that 'harmonic analysis can handle systems of complexity one'. For a variety of reasons, however, it is not immediately applicable to an understanding of the quantity

$$\sum \Lambda(\psi_1(\vec{n}))\dots\Lambda(\psi_d(\vec{n})) \tag{3.5}$$

appearing in Dickson's Conjecture. One obvious point is that the average in Proposition 3.0.7 is over $(\mathbb{Z}/N\mathbb{Z})^d$, rather than over $[N]^d$ or over the lattice points inside a convex body. This is a purely technical distinction, and is dealt with in [24, Appendix C].

A more serious problem arises from consideration of how Proposition 3.0.7 might be applied. There is certainly no mileage to be gained from applying it in the most naïve way, that is to say with $f_1 = \dots = f_t = \Lambda$. Indeed in that case condition (3.2) does hold (with $r = 0$), and so we cannot rule out the possibility of (3.1) holding (and, of course, Dickson's Conjecture predicts that (3.1) does hold much of the time). To eliminate the possibility of (3.2) holding with $r = 0$ we might split $\Lambda = 1 + (\Lambda - 1)$, expand (3.5) as a sum of 2^t terms, and use Proposition 3.0.7 to show that all of the terms except the one with $f_1 = \dots = f_t = 1$ are 'negligible'. This also fails to work, for the simple reason that those other terms may not be negligible. Indeed if they were then the arithmetic constant in Dickson's Conjecture would be simply 1 rather than the product $\beta_\infty \prod_p \beta_p$ reflecting the distribution of primes (mod 2), (mod 3) etc.

In all of the the work of the author and Tao on primes these issues are bypassed by means of the so-called W-trick. The trick is easiest to describe in the context of our paper [21] establishing the existence of arbitrarily long progressions of primes. Look at the primes $2, 3, 5, 7, \dots$. They are very irregularly distributed (mod 2). However if one deletes the element 2 and rescales the remaining primes by the map $x \mapsto (x-1)/2$ one ends up with the sequence $1, 2, 3, 5, 6, 8, \dots$. This is now quite regularly distributed (mod 2), because there are roughly the same number of primes congruent to 1(mod 4) as there are primes congruent to 3(mod 4). Furthermore if one finds a long arithmetic

progression in the new sequence it translates immediately to a long progression in the primes.

Unfortunately, however, this new sequence is not well-distributed (mod 3), as the only element congruent to 1(mod 3) that it contains is 1. However we could pick out the elements divisible by 3, that is to say $3, 6, 9, 15, \dots$ and divide through by 3 to obtain the new sequence $1, 2, 3, 5, \dots$. This is now well-distributed modulo both 2 and 3.

The process may be continued with the primes up to some threshold $w(N)$. Choosing $w(N)$ to tend to infinity with N, the resulting sequences have no appreciable biases in small modulo small numbers.

It is in fact quite easy to formalise this idea and to see how it may be applied to quite general problems such as (3.5). The sequences that result from the sieving process we have just described are of the form

$$\{n : Wn + b \quad \text{is prime}\}$$

where $W := 2 \times 3 \times \cdots \times w(N)$ (hence the name 'W-trick') and $(b, W) = 1$. For consideration of the weighted sum appearing in (3.5) it is rather natural to introduce the functions

$$\Lambda_{b,W}(n) := \frac{\phi(W)}{W}\Lambda(Wn + b),$$

which have average value roughly 1. Roughly speaking, the sum in (3.5) may be split into $\phi(W)^t$ sums of the form

$$\sum \Lambda_{b_1,W}(\tilde{\psi_1}(\vec{n})) \dots \Lambda_{b_t,W}(\tilde{\psi_d}(\vec{n})) \tag{3.6}$$

(for the details of this decomposition see [24, Chapter 5]). One might then attempt to evaluate each of these by splitting

$$\Lambda_{b_i,W} = 1 + (\Lambda_{b_i,W} - 1)$$

and then apply Proposition 3.0.7 to show that all of the terms except that with $f_1 = \cdots = f_t = 1$ are negligible.

Such an approach is promising, but there is one serious additional problem. Proposition 3.0.7 only applied, as we stated it, to functions f_i which are bounded by 1. The functions $\Lambda_{b_i,W} - 1$ are certainly not bounded by one. Indeed, the harmonic analysis argument leading up to (3.4) relied on this boundedness in a rather essential way.

It turns out that there *is* a version of Proposition 3.0.7 which applies to functions which are not necessarily bounded by 1; this is one of the main results of [24], and the key idea was also an important component of our earlier work [21].

For simplicity let us think about the von Mangoldt function Λ itself, rather than the 'W-tricked' variants $\Lambda_{b,W}$. Let $R = N^\gamma$, where $\gamma \in (0, 1)$ is a real number, and let us recall the discussion of §1, where we observed that

$$\frac{1}{(\log R)^2}\Lambda_R^2(n) = \big(\sum_{\substack{d|n\\ d\leqslant R}} \lambda_d^{\mathrm{GY}}\big)^2$$

is a sensible majorant for the characteristic function of the primes between R and N, where

$$\lambda_d^{\mathrm{GY}} := \mu(d)\frac{\log(R/d)}{\log R}.$$

It follows the function

$$\nu(n) := \frac{1}{\log N}\big(\sum_{\substack{d|n\\ d\leqslant R}} \lambda_d^{\mathrm{GY}}\big)^2$$

essentially majorizes some multiple $C_\gamma\Lambda(n)$ of the von Mangoldt function on the interval $[N]$ (where by *essentially* we mean that there may be problems when $n \leqslant R$ or n is a prime power, but these are highly unimportant exceptions). We note that the link we have just made to the work of Goldston, Pintz and Yıldırım is by no means artificial; indeed a crucial moment in the development of [21] occurred when Andrew Granville drew our attention to [9].

The weights ν are much more flexible than Λ, since it is possible to evaluate such sums as

$$\mathbb{E}_{n\leqslant N}\nu(n)\nu(n+2)$$

asymptotically by variants of the computations leading to (1.3). As in those computations the key feature is that by choosing the parameter γ to be small enough the number of terms which result from expanding out the sums over d is small enough that error terms do not dominate.

In fact (after an application of the W-trick discussed above and with an appropriate choice of $\gamma = \gamma(t,d)$) the weights are sufficiently flexible that they may be shown to satisfy two technical conditions called the *linear forms* and *correlation* conditions. These conditions were introduced in [21, §3], and the variants of these conditions appropriate for a discussion of Dickson's Conjecture are given in [24, §6]. As a result of this the weight ν qualifies to be called *pseudorandom*.

As the reader may have guessed from the above discussion, it is possible to prove a version of Proposition 3.0.7 in which the condition that the f_i take values in $[-1,1]$ is relaxed to a condition $|f_i(x)| \leqslant \nu(x)$, where ν is a pseudorandom weight function. The first step is to establish 'generalized von Neumann'-type results in which the functions f_i are bounded by ν, rather than just by 1. Specifically, one deduces from an assumption (3.1) that each of the Gowers norms $\|f_i\|_{U^2}$ is somewhat large. This is once again accomplished by several applications of the Cauchy-Schwarz inequality, but the presence of the weight ν makes the details even more complicated. For a fully worked-out example, see [21, §5]. Once this is done one must establish an inverse theorem for the Gowers U^2-norm for functions f with $|f(x)| \leqslant \nu(x)$. As we remarked, some new ideas are required here since the harmonic analysis argument leading up to (3.4) breaks down if f is not bounded by one.

In fact this inverse theorem is deduced from the version with $|f_i(x)| \leqslant 1$ by means of the following decomposition result, which is [24, Proposition 10.3].

Lemma 3.0.8 (Decomposition)**.** *Suppose that $\nu : \mathbb{Z}/N\mathbb{Z} \to \mathbb{R}_{\geqslant 0}$ is a pseudorandom measure, and that $f : \mathbb{Z}/N\mathbb{Z} \to \mathbb{R}$ is a function with $|f(x)| \leqslant \nu(x)$ for all x. Then we may decompose*

$$f = f_1 + f_2$$

where $|f_1(x)| \leqslant 1$ for all x and $\|f_2\|_{U_2} = o(1)$ as $N \to \infty$.

We shall almost nothing about the proof of this result, but it is also one of the key ingredients in [21]. For a discussion, see [43, §6]. For a broader discussion of the 'energy-increment' strategy used in the proof, which appears in many different contexts in additive combinatorics, see [45].

Suppose that $|f(x)| \leqslant \nu(x)$ and that $\|f\|_{U^2} \geqslant \delta$. Applying Lemma 3.0.8, we see that $\|f_1\|_{U^2} \geqslant \delta/2$. By the inverse theorem for the U^2-norm of bounded functions, there is some $r \in \mathbb{Z}/N\mathbb{Z}$ such that

$$|\mathbb{E}_{n \in \mathbb{Z}/N\mathbb{Z}} f_1(n) e(-rn/N)| \geqslant \delta^2/4.$$

However by the converse of the inverse theorem and the fact that $\|f_2\|_{U^2} = o(1)$ we see that

$$|\mathbb{E}_{n \in \mathbb{Z}/N\mathbb{Z}} f_2(n) e(-rn/N)| = o(1)$$

(Note that the proof of this converse result did not require f_2 to be bounded by 1). By the triangle inequality it follows that

$$|\mathbb{E}_{n \in \mathbb{Z}/N\mathbb{Z}} f(n) e(-rn/N)| \geqslant \delta^2/4 - o(1) \geqslant \delta^2/8,$$

which concludes the 'transference' of the inverse theorem for the U^2-norm from functions bounded by 1 to functions bounded by ν.

Let us take stock of our position. We have indicated a proof of Proposition 3.0.7 when the functions f_i are bounded by a pseudorandom weight ν, a fairly robust realisation of the principle that harmonic analysis governs the behaviour of systems of complexity one. We have split the von Mangoldt function Λ into functions $\Lambda_{b,W}$, and rewritten the sum which interests us, namely (3.5), as a sum of expressions of the form (3.6). To evaluate these we effect the further splitting $\Lambda_{b,W} = 1 + (\Lambda_{b,W} - 1)$, and hope to show that any sum

$$\sum f_1(\tilde{\psi}_1(\vec{n})) \dots f_t(\tilde{\psi}_t(\vec{n}))$$

in which at least one f_i equals $\Lambda_{b,W} - 1$ is negligible. All of these functions are essentially dominated by some pseudorandom weight ν of the type considered by Goldston and Yıldırım, and so by our robust version of Proposition 3.0.7 it suffices to rule out the possiblity that $\Lambda_{b,W} - 1$ correlates with a linear phase function; that is to say, we must establish that

$$|\mathbb{E}_{n \leqslant N} (\Lambda_{b,W}(n) - 1) e(-rn/N)| = o(1). \tag{3.7}$$

This estimate may be established in a fairly classical fashion using the ideas of Hardy, Littlewood and Vinogradov. In [24] we proceed by first effecting some further decompositions, in keeping with our general philosophy that problems should be 'transferred'

to a situation where functions are bounded by 1. We skip the details (which may be found in [24, §12]) and merely state that (3.7) can be deduced from the estimate

$$|\mathbb{E}_{n\leqslant N}\mu(n)e(-rn/N)| \ll_A \log^{-A} N, \tag{3.8}$$

for some suitably large A. That such an estimate holds (with *any* A) is a well-known result of Davenport [5]. To prove it one may use the method of Type I/Type II sums discussed in §2. In fact, Propositon 2.3.1 is true with the von Mangoldt function Λ replaced by the Möbius function μ. The proof is almost the same, relying on a decomposition of μ which is very similar to Vaughan's decomposition of Λ.

The remarks following the statement of Proposition 2.3.1 are particularly relevant here. We can hope that the method of Type I/II sums will be effective in bounding (3.8) unless r/N is approximately a/q, for some small q (that is, the method ought to be successful in the 'minor arc' case). Luckily in the 'major arc' case one may approximate $e(-rn/N)$ by the sum of a few Dirichlet characters to modulus q. The resulting sums $\sum_{n\leqslant N}\mu(n)\chi(n)$ may then be estimating using standard techniques of analytic number theory together with information about the non-existence of zeros near $\Re s = 1$ of the L-functions $L(s,\chi)$: for details see [32, Prop 5.29].

This concludes our discussion of a proof of Dickson's Conjecture for systems of complexity one. As we have remarked, this result could also be obtained by a more classical application of the circle method. However it turns out that large parts of our discussion adapt very painlessly to systems of complexity $s > 1$, whereas this does not seem to be the case for the classical techniques.

One has, for example, the following bound of generalized von Neumann type:

$$|\mathbb{E}_{\vec{n}\in(\mathbb{Z}/N\mathbb{Z})^d} f_1(\psi_1(\vec{n}))\dots f_t(\psi_t(\vec{n}))| \leqslant \inf_{i\in[t]} \|f_i\|_{U^{s+1}} \tag{3.9}$$

for systems $\psi_1,\dots,\psi_t$ of complexity s, where $\|f\|_{U^k}$ is the *Gowers U^k-norm* of f and is defined by

$$\|f\|_{U^k}^{2^k} := \mathbb{E}_{x,h_1,\dots,h_k} \prod_{\omega_1,\dots,\omega_k\in\{0,1\}} f(x+\omega_1 h_1+\dots+\omega_k h_k)$$

(with complex conjugates being taken of the terms with an odd number of h_is). This is true even if the functions f_i are only bounded by a pseudorandom weight ν. A statement very close to (3.9) is proved in [24, Appendix C].

The decomposition result, Lemma 3.0.8, also adapts in a fairly painless manner.

The first really serious issue that we encounter is in finding a generalization of the inverse theorem for the U^2-norm. If $f : \mathbb{Z}/N\mathbb{Z} \to [-1,1]$ is a function such that $\|f\|_{U^3} \geqslant \delta$, what can be said? The most immediate difficulty with attacking this statement is the lack of a suitable formula generalizing the relation $\|f\|_{U^2} = \|\hat{f}\|_4$. A more decisive problem is revealed by consideration of the function $f(n) = e(n^2/N)$. One may check that $\|f\|_{U^3} = 1$ (this is essentially a manifestation of the fact that the third derivative of a quadratic is zero). With somewhat more effort one may check that this f does not have substantial correlation with a *linear* exponential $e(rn/N)$. Thus an inverse

theorem for the U^3-norm must encode some kind of 'higher harmonic analysis' which takes account of these quadratic phases as well as just linear ones. The situation is further complicated by the existence of further examples, such as $f(n) = e(n[n\sqrt{2}]/N)$, for which $\|f\|_{U^3}$ is large, but for which f does not even exhibit genuine quadratic behaviour. A full discussion of examples related to these may be found in [17].

It turns out that these two examples, $f(n) = e(n^2/N)$ and $f(n) = e(n[n\sqrt{2}]/N)$, can both be interpreted as objects living on a 2-*step nilmanifold*, that is to say a quotient G/Γ where G is a 2-step nilpotent Lie group and Γ is a discrete and cocompact subgroup. The archetypal example is the Heisenberg example in which

$$G = \begin{pmatrix} 1 & \mathbb{R} & \mathbb{R} \\ 0 & 1 & \mathbb{R} \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad \Gamma = \begin{pmatrix} 1 & \mathbb{Z} & \mathbb{Z} \\ 0 & 1 & \mathbb{Z} \\ 0 & 0 & 1 \end{pmatrix}.$$

Quadratic polynomials appear quite naturally in such a group G, for instance in the computation

$$\begin{pmatrix} 1 & \alpha & \beta \\ 0 & 1 & \gamma \\ 0 & 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & n\alpha & n\beta + \frac{1}{2}n(n-1)\alpha\gamma \\ 0 & 1 & n\gamma \\ 0 & 0 & 1 \end{pmatrix}.$$

Taking such a sequence of matrices and postmultiplying by elements of Γ so that all of the entries lie between $[-1/2, 1/2]^3$ (that is, reducing to a fundamental domain for the action of Γ on G) one soon sees the appearance of the more complicated 'bracket quadratics' $\gamma n[\alpha n]$ too. A fuller discussion, with motivating remarks, may be found in [17].

What is more, correlation with an example arising in this setting is the *only* way in which a function f can have large U^3-norm. This is the inverse theorem for the U^3-norm, proved in [22] building on ideas of Gowers [15]. It is conjectured that an analogous result holds for the U^{s+1}-norm in general, a conjecture we refer to as the *Gowers Inverse conjecture* GI(s).

Conjecture 3.0.9 (Gowers inverse conjecture GI(s))**.** *Suppose that $f : \mathbb{Z}/N\mathbb{Z} \to [-1, 1]$ is a function and that $\|f\|_{U^{s+1}} \geqslant \delta$. Then there is an s-step nilmanifold G/Γ, a Lipschitz function $F : G/\Gamma \to [-1, 1]$ and elements $g \in G$, $x \in G/\Gamma$ such that*

$$|\mathbb{E}_{n \leqslant N} f(n)F(g^n x\Gamma)| \gg_\delta 1.$$

The dimension and complexity of G/Γ and the Lipschitz constant of F are all $O_\delta(1)$.

The function $n \mapsto F(g^n x\Gamma)$ is called an s-step nilsequence. To state this conjecture properly one must of course define the notion of 'complexity', and also assign a metric to G/Γ so that the notion of Lipschitz constant may be properly formalised. A version of the conjecture was first formulated in [24, §8]. There, a metric on G/Γ was assigned quite arbitrarily. With the benefit of hindsight it is probably better to proceed as in our more recent paper [25, §2], in which the notions of 'complexity' and 'metric' are both developed from the notion of a *Mal'cev basis* for G/Γ.

The precise statements are not important in order to understand the philosophy which lies behind Conjecture 3.0.9 and its interplay with the generalized von Neumann theorem (3.9): it seems as though the correct 'harmonics' with which to study systems $\{\psi_1, \dots, \psi_t\}$ of complexity s are the s-step nilsequences.

Conjecture 3.0.9 is known when $s = 1$, and we proved it earlier. Note that the linear exponentials $n \mapsto e(-rn/N)$ may easily be interpreted as 1-step nilsequences living on the nilmanifold $\mathbb{R}/\mathbb{Z}$. As we stated, it is also known when $s = 2$, this being the main result of [22]. Tao and I hope to report progress on the general case $s \geqslant 3$ in the near future.

Assuming Conjecture 3.0.9, one may start to work through the proof of Dickson's Conjecture in the complexity 1 case and attempt to generalise it to the complexity s situation. Replacing occurrences of linear exponentials $e(-rn/N)$ by s-step nilsequences $F(g^n x\Gamma)$, the argument runs with remarkably few changes. One fairly significant extra difficulty occurs in the proof of Lemma 3.0.8, where a 'converse' to the inverse conjecture is required. Namely, one needs to know that if

$$|\mathbb{E}_{n\leqslant N} f(n)F(g^n x\Gamma)| \geqslant \delta$$

for some s-step nilsequence $F(g^n x\Gamma)$ then

$$\|f\|_{U^{s+1}} \gg_\delta 1,$$

where the implied constant may also depend on the complexity of G/Γ and on the Lipschitz constant of F. Such a result is already present in [22, §14], and a somewhat more conceptual proof is given in [24, Appendix E]. Both of these appendices were based on extensive conversations with members of the ergodic theory community.

By far the most serious obstacle is the last one, where we reduce to establishing a generalization of (3.8) for nilsequences. In other words we seek the bound

$$|\mathbb{E}_{n\leqslant N}\mu(n)F(g^n x\Gamma)| \ll_A \log^{-A} N$$

for all $A > 0$, where $F(g^n x\Gamma)$ is an s-step nilsequence arising from some s-step nilmanifold G/Γ, and the implied constant may also depend on the complexity of G/Γ and the Lipschitz constant of F. This bound is referred to as the Möbius and Nilsequences Conjecture MN(s). As we remarked, the conjecture MN(1) was essentially established by Davenport. The case MN(2) was obtained in the paper [23]. The general case MN(s) has recently been resolved by the authors and will appear in the short paper [26]; the key technical ingredient in that proof is the main result of [25], which may be thought of as a kind of generalization of the major-minor arc decomposition to nilsequences of arbitrary step. The method of Type I/II sums is crucial once more.

The reader wishing to study any of this work might find the following table helpful. Let me once again emphasise that the purpose of this article has been to guide potential readers through the papers [21, 22, 23, 24, 25] and [26]; we do not intend to suggest that there is no other work going on in the subject!

[21], *The primes contain arbitrarily long arithmetic progressions,* independent of the other papers except it contains the proof of Decomposition Lemma 3.0.8.

[22], *An inverse theorem for the Gowers U^3-norm, with applications*, proof of the GI(2) conjecture.

[23], *Quadratic Uniformity of the Möbius function,* proof of the MN(2) conjecture, to be largely superceded by [26] but, unlike that paper, can be understood without [25].

[24], *Linear Equations in primes,* proof that the GI(s) and MN(s) conjectures together imply Dickson's conjecture for systems $\{\psi_1, \dots, \psi_t\}$ of complexity s. The discussion in this article has been largely an exposition of some of the ideas in this paper.

[25], *The Quantitative Behaviour of Polynomial Orbits on Nilmanifolds,* key technical ingredient for studying nilsequences

[26], *The Möbius and Nilsequences Conjectures,* proof of MN(s) conjecture for all s, heavily reliant on [25].

References

[1] *Problems from the ARCC Workshop "Gaps between primes"*, ed. A. Kumchev, available at `http://www.aimath.org/WWN/primegaps/primegaps.pdf`.
[2] M. Agwaral, N. Kayal and N. Saxena, *PRIMES is in P*, Ann. Math. **160** (2004), 781–793.
[3] A. Balog, *Linear equations in primes,* Mathematika **39** (1992), no. 2, 367–378.
[4] E. Bombieri and H. Davenport, *Small differences between prime numbers*, *Proc. Roy. Soc. Ser. A* **293** (1966), 1–18.
[5] H. Davenport, *On some infinite series involving arithmetical functions, II,* Quart. J. Math. Oxford **8** (1937), 313–320.
[6] W. Duke, J. B. Friedlander and H. Iwaniec, *Equidistribution of roots of a quadratic congruence to prime moduli,* Ann. of Math. (2) **141** (1995), no. 2, 423–441.
[7] P.D.T.A Elliott and H. Halberstam, *A conjecture in prime number theory,* Symposia Mathematica **4** (INDAM, Rome, 1968/69) 59–72, Academic Press, London.
[8] P. Erdős, The difference of consecutive primes, *Duke Math. J.* **6** (1940), 438–441.
[9] D. Goldston and C. Y. Yıldırım , *Small gaps between primes, I,* available at `http://www.arxiv.org/abs/math/0504336`.
[10] D. A. Goldston, J. Pintz and C. Y. Yıldırım, *Primes in tuples II,* in preparation.
[11] D. A. Goldston, S. W. Graham, J. Pintz and C. Y. Yıldırım, *Small gaps between primes or almost primes,* preprint available at `http://www.arxiv.org/abs/math/0506067`.
[12] D. A. Goldston, J. Pintz and C. Y. Yıldırım, *The path to recent progress on small gaps between primes,* preprint available at `http://www.arxiv.org/abs/math/0512436`.
[13] D. A. Goldston, J. Pintz and C. Y. Yıldırım, *Primes in tuples I,* preprint available at `http://www.arxiv.org/abs/math/0508185`.
[14] D. A. Goldston, Y. Motohashi, J. Pintz and C. Y. Yıldırım, *Small gaps between primes exist,* preprint available at `http://www.arxiv.org/abs/math/0505300`.
[15] W. T. Gowers, *A new proof of Szemerédi's theorem for arithmetic progressions of length four,* Geom. Funct. Anal. **8** (1998), no. 3, 529–551.
[16] A. Granville, *A good new millenium for the primes,* The Madrid Intelligencer (2006) pages 32–36. Also available on the author's webpage.
[17] B. J. Green, *Generalizing the Hardy-Littlewood method for primes,* Proceedings of the International Congress of Mathematicians 2006 (Madrid), vol. 2,
[18] ———, *Montréal Lecture notes on Quadratic Fourier Analysis,* to appear in Proceedings of the CMS-Clay School on Additive Combinatorics, Montréal 2006.
[19] ———, *Long arithmetic progressions of primes,* in Analytic Number Theory: A tribute to Gauss and Dirichlet, CMI/AMS 2007.
[20] B. J. Green and T. C. Tao, *Restriction theory of the Selberg sieve, with applications,* Jour. Th. Nombres Bordeaux **18** (2006), 147–182.

[21] ———, *The primes contain arbitrarily long arithmetic progressions,* to appear in Ann. Math., preprint available at `http://www.arxiv.org/abs/math/0404188`.
[22] ———, *An inverse theorem for the Gowers U^3-norm, with applications*, to appear in Proc. Edinburgh Math. Soc, preprint available at `http://www.arxiv.org/abs/math/0503014`.
[23] ———, *Quadratic Uniformity of the Möbius function,* to appear in Annales de l'Institut Fourier, Grenoble, preprint available at `http://www.arxiv.org/abs/math/0606087`.
[24] ———, *Linear Equations in primes,* to appear in Ann. Math, preprint available at `http://www.arxiv.org/abs/math/0606088`.
[25] ———, *The Quantitative Behaviour of Polynomial Orbits on Nilmanifolds,* preprint available at `http://www.arxiv.org/abs/0709.3562`.
[26] ———, *The Möbius and Nilsequences Conjectures,* in preparation.
[27] G. H. Hardy and J. E. Littlewood, unpublished manuscript, see [39].
[28] B. Host, *Progressions arithmétiques dans les nombres premiers, d'après B. Green et T. Tao,* Seminaire Bourbaki,Mars 2005, 57eme annee, 2004-2005, no. 944.
[29] M. N. Huxley, On the differences of primes in arithmetical progressions, *Acta Arith.* **15** (1968/69), 367–392.
[30] ———, *Small differences between consecutive primes II,* Mathematika **24** (1977), 142–152.
[31] ———, *An application of the Fouvry-Iwaniec theorem*, Acta Arith. **43** (1984), 441–443.
[32] H. Iwaniec and E. Kowalski, *Analytic number theory,* AMS Colloq. Math. **53**, Providence RI 2004.
[33] B. Kra, *The Green-Tao theorem on arithmetic progressions in the primes: an ergodic point of view,* Bull. Amer. Math. Soc. (N.S.) **43** (2006), no. 1, 3–23.
[34] A. V. Kumchev, A. V. and D. I. Tolev, *An invitation to additive prime number theory,* Serdica Math. J. **31** (2005), no. 1-2, 1–74.
[35] H. Maier, Small differences between prime numbers, *Michigan Math. J.* **35** (1988), 323–344.
[36] C. Mauduit et J. Rivat, *Sur un probléme de Gelfond: la somme des chiffres des nombres premiers,* preprint.
[37] M. B. Nathanson, *Additive number theory: The classical bases*, Graduate Texts in Mathematics **164**. Springer-Verlag, New York, 1996. xiv+342 pp.
[38] G. Z. Pilt'ai, *On the size of the difference between consecutive primes*, Issledovania po teorii chisel, **4** (1972), 73–79.
[39] R. A. Rankin, The difference between consecutive prime numbers. II, *Proc. Cambridge Philos. Soc.* **36** (1940), 255–266.
[40] G. Ricci, Sull'andamento della differenza di numeri primi consecutivi, *Riv. Mat. Univ. Parma* **5** (1954), 3–54.
[41] K. Soundararajan, *Small gaps between prime numbers: The work of Goldston-Pintz-Yıldırım,* Bull. Amer. Math. Soc. **44** (2007), 1–18.
[42] T. C. Tao, *The dichotomy between structure and randomness, arithmetic progressions, and the primes,* Proceedings of the International Congress of Mathematicians, Madrid 2006, Vol. I., 581–608.
[43] ———, Obstructions to uniformity, and arithmetic patterns in the primes Quarterly J. Pure Appl. Math. 2 (2006), 199-217 [Special issue in honour of John H. Coates, Vol. 1 of 2]
[44] ———, *Arithmetic progressions and the primes,* El Escorial lectures, Collectanea Mathematica (2006), Vol. Extra., 37-88. [Proceedings, 7th International Conference on Harmonic Analysis and Partial Differential Equations]
[45] ———, *Structure and randomness in combinatorics,* submitted to FOCS (Foundations of Computer Science) 2007.
[46] T. C. Tao and V. H. Vu, *Additive Combinatorics,* Cambridge Studies in Advanced Mathematics **105**, CUP 2006.
[47] S. Uchiyama, *On the difference between consecutive prime numbers,* Acta Arith. **27** (1975), 153–157.
[48] R. C. Vaughan, *Sommes trigonométriques sur les nombres premiers,* C. R. Acad. Sci. Paris Sér. A-B **285** (1977), no. 16, A981–A983.

Centre for Mathematical Sciences, Wilberforce Road, Cambridge CB3 0WA, England

E-mail address: b.j.green@dpmms.cam.ac.uk