The ternary Goldbach problem

Harald Andrés Helfgott

Abstract. The ternary Goldbach conjecture, or three-primes problem, states that every odd number n greater than 5 can be written as the sum of three primes. The conjecture, posed in 1742, remained unsolved until now, in spite of great progress in the twentieth century. In 2013 – following a line of research pioneered and developed by Hardy, Littlewood and Vinogradov, among others – the author proved the conjecture. In this, as in many other additive problems, what is at issue is really the proper usage of the limited information we possess on the distribution of prime numbers. The problem serves as a test and whetting-stone for techniques in analysis and number theory – and also as an incentive to think about the relations between existing techniques with greater clarity. We will go over the main ideas of the proof. The basic approach is based on the circle method, the large sieve and exponential sums. For the purposes of this overview, we will not need to work with explicit constants; however, we will discuss what makes certain strategies and procedures not just effective, but efficient, in the sense of leading to good constants. Still, our focus will be on qualitative improvements.

Mathematics Subject Classification (2010). Primary 11P32.

Keywords. Analytic number theory, additive problems, prime numbers.

The question we will discuss, or one similar to it, seems to have been first posed by Descartes, in a manuscript published only centuries after his death [14, p. 298]. Descartes states: "Sed & omnis numerus par fit ex uno vel duobus vel tribus primis" ("But also every even number is made out of one, two or three prime numbers.") This statement comes in the middle of a discussion of sums of polygonal numbers, such as the squares.

Statements on sums of primes and sums of values of polynomials (polygonal numbers, powers n^k, etc.) have since shown themselves to be much more than mere curiosities – and not just because they are often very difficult to prove. Whereas the study of sums of powers can rely on their algebraic structure, the study of sums of primes leads to the realization that, from several perspectives, the set of primes behaves much like the set of integers – and that this is truly hard to prove.

If, instead of the primes, we had a random set of odd integers S whose density – an intuitive concept that can be made precise – equaled that of the primes, then we would expect to be able to write every odd number as a sum of three elements of S, and every even number as the sum of two elements of S. We would have to check by hand whether this is true for small odd and even numbers, but it is relatively easy to show that, after a long enough check, it would be very unlikely that there would be any exceptions left among the infinitely many cases left to check.

The question, then, is in what sense we need the primes to be like a random set of integers; in other words, we need to know what we can prove about the regularities of the

Proceedings of the International Congress of Mathematicians, Seoul, 2014

distribution of the primes. This is one of the main questions of analytic number theory; progress on it has been very slow and difficult. Thus, the real question is how to use well the limited information we do have on the distribution of the primes.

1. History and new developments

The history of the conjecture starts properly with Euler and his close friend, Christian Goldbach, both of whom lived and worked in Russia at the time of their correspondence – about a century after Descartes' isolated statement. Goldbach, a man of many interests, is usually classed as a serious amateur; he seems to have awakened Euler's passion for number theory, which would lead to the beginning of the modern era of the subject [71, Ch. 3, §IV]. In a letter dated June 7, 1742 – written partly in German, partly in Latin – Goldbach made a conjectural statement on prime numbers, and Euler rapidly reduced it to the following conjecture, which, he said, Goldbach had already posed to him: every positive integer can be written as the sum of at most three prime numbers.

We would now say "every integer greater than 1", since we no long consider 1 to be a prime number. Moreover, the conjecture is nowadays split into two:

- the *weak*, or ternary, Goldbach conjecture states that every odd integer greater than 5 can be written as the sum of three primes;
- the *strong*, or binary, Goldbach conjecture states that every even integer greater than 2 can be written as the sum of two primes.

As their names indicate, the strong conjecture implies the weak one (easily: subtract 3 from your odd number n, then express $n-3$ as the sum of two primes).

The strong conjecture remains out of reach. A short while ago – the first complete version appeared on May 13, 2013 – the present author proved the weak Goldbach conjecture.

Main Theorem. *Every odd integer greater than* 5 *can be written as the sum of three primes.*

The proof is contained in the preprints [28], [27], [29]. It builds on the great progress towards the conjecture made in the early 20th century by Hardy, Littlewood and Vinogradov. In 1937, Vinogradov proved [67] that the conjecture is true for all odd numbers n larger than some constant C. (Hardy and Littlewood had shown the same under the assumption of the Generalized Riemann Hypothesis, which we shall have the chance to discuss later.)

It is clear that a computation can verify the conjecture only for $n \leq c$, c a constant: computations have to be finite. What can make a result coming from analytic number theory be valid only for $n \geq C$?

An analytic proof, generally speaking, gives us more than just existence. In this kind of problem, it gives us more than the possibility of doing something (here, writing an integer n as the sum of three primes). It gives us a rigorous estimate for the number of ways in which this *something* is possible; that is, it shows us that this number of ways equals

$$\text{main term} + \text{error term}, \tag{1.1}$$

where the main term is a precise quantity $f(n)$, and the error term is something whose absolute value is at most another precise quantity $g(n)$. If $f(n) > g(n)$, then (1.1) is nonzero, i.e., we will have shown that the existence of a way to write our number as the sum of three primes.

(Since what we truly care about is existence, we are free to weigh different ways of writing n as the sum of three primes however we wish – that is, we can decide that some primes "count" twice or thrice as much as others, and that some do not count at all.)

Typically, after much work, we succeed in obtaining (1.1) with $f(n)$ and $g(n)$ such that $f(n) > g(n)$ asymptotically, that is, for n large enough. To give a highly simplified example: if, say, $f(n) = n^2$ and $g(n) = 100n^{3/2}$, then $f(n) > g(n)$ for $n > C$, where $C = 10^4$, and so the number of ways (1.1) is positive for $n > C$.

We want a moderate value of C, that is, a C small enough that all cases $n \leq C$ can be checked computationally. To ensure this, we must make the error term bound $g(n)$ as small as possible. This is our main task. A secondary (and sometimes neglected) possibility is to rig the weights so as to make the main term $f(n)$ larger in comparison to $g(n)$; this can generally be done only up to a certain point, but is nonetheless very helpful.

As we said, the first unconditional proof that odd numbers $n \geq C$ can be written as the sum of three primes is due to Vinogradov. Analytic bounds fall into several categories, or stages; quite often, successive versions of the same theorem will go through successive stages.

1. An *ineffective* result shows that a statement is true for some constant C, but gives no way to determine what the constant C might be. Vinogradov's first proof of his theorem (in [67]) is like this: it shows that there exists a constant C such that every odd number $n > C$ is the sum of three primes, yet gives us no hope of finding out what the constant C might be.[1] Many proofs of Vinogradov's result in textbooks are also of this type.
2. An *effective*, but not explicit, result shows that a statement is true for some unspecified constant C in a way that makes it clear that a constant C could in principle be determined following and reworking the proof with great care. Vinogradov's later proof ([68], translated in [69]) is of this nature. As Chudakov [8, §IV.2] pointed out, the improvement on [67] given by Mardzhanishvili [41] already had the effect of making the result effective.[2]
3. An *explicit* result gives a value of C. According to [8, p. 201], the first explicit version of Vinogradov's result was given by Borozdkin in his unpublished doctoral dissertation, written under the direction of Vinogradov (1939): $C = \exp(\exp(\exp(41.96)))$. Such a result is, by definition, also effective. Borodzkin later [2] gave the value $C = e^{e^{16.038}}$, though he does not seem to have published the proof. The best – that is, smallest – value of C known before the present work was that of Liu and Wang [40]: $C = 2 \cdot 10^{1346}$.
4. What we may call an *efficient* proof gives a reasonable value for C – in our case, a value small enough that checking all cases up to C is feasible.

How far were we from an efficient proof? That is, what sort of computation could ever be feasible? The number of picoseconds since the beginning of the universe is less than 10^{30}, whereas the number of protons in the observable universe is currently estimated at

[1] Here, as is often the case in ineffective results in analytic number theory, the underlying issue is that of *Siegel zeros*, which are believed not to exist, but have not been shown not to; the strongest bounds on (i.e., against the existence of) such zeros are ineffective, and so are all of the many results using such estimates.

[2] The proof in [41] combined the bounds in [67] with a more careful accounting of the effect of the single possible Siegel zero within range.

$\sim 10^{80}$. This means that even a parallel computer the size of the universe could never perform a computation requiring 10^{110} steps, even if it ran for the age of the universe. Thus, $C = 2 \cdot 10^{1346}$ is too large.

I gave a proof with $C = 10^{29}$ in May 2013. Since D. Platt and I had verified the conjecture for all odd numbers up to $n \leq 8.8 \cdot 10^{30}$ by computer [31], this established the conjecture for all odd numbers n.

(In December 2013, C was reduced to 10^{27} [29]. The verification of the ternary Goldbach conjecture up to $n \leq 10^{27}$ can be done in a home computer over a weekend. All must be said: this uses the verification of the binary Goldbach conjecture for $n \leq 4 \cdot 10^{18}$ [46], which itself required computational resources far outside the home-computing range. Checking the conjecture up to $n \leq 10^{27}$ was not even the main computational task that needed to be accomplished to establish the Main Theorem – that task was the finite verification of zeros of L-functions in [48], a general-purpose computation that should be useful elsewhere. We will discuss the procedure at the end of the article.)

What was the strategy of [27–29]? The basic framework is the one pioneered by Hardy and Littlewood for a variety of problems – namely, the *circle method*, which, as we shall see, is an application of Fourier analysis over $\mathbb{Z}$. (There are other, later routes to Vinogradov's result; see [21, 24] and especially the recent work [57], which avoids using anything about zeros of L-functions inside the critical strip.) Vinogradov's proof, like much of the later work on the subject, was based on a detailed analysis of exponential sums, i.e., Fourier transforms over $\mathbb{Z}$. So is the proof that we will sketch.

At the same time, the distance between $2 \cdot 10^{1346}$ and 10^{27} is such that we cannot hope to get to 10^{27} (or any other reasonable constant) by fine-tuning previous work. Rather, we must work from scratch, using the basic outline in Vinogradov's original proof and other, initially unrelated, developments in analysis and number theory (notably, the large sieve). Merely improving constants will not do; we must do qualitatively better than previous work (by non-constant factors) if we are to have any chance to succeed. It is on these qualitative improvements that we will focus.

* * *

It is only fair to review some of the progress made between Vinogradov's time and ours. Here we will focus on results; later, we will discuss some of the progress made in the techniques of proof. For a fuller account up to 1978, see R. Vaughan's ICM lecture notes on the ternary Goldbach problem [65].

In 1933, Schnirelmann proved [56] that every integer $n > 1$ can be written as the sum of at most K primes for some unspecified constant K. (This pioneering work is now considered to be part of the early history of additive combinatorics.) In 1969, Klimov gave an explicit value for K (namely, $K = 6 \cdot 10^9$); he later improved the constant to $K = 115$ (with G. Z. Piltay and T. A. Sheptickaja) and $K = 55$. Later, there were results by Vaughan [63] ($K = 27$), Deshouillers [15] ($K = 26$) and Riesel-Vaughan [54] ($K = 19$).

Ramaré showed in 1995 that every even number $n > 1$ can be written as the sum of at most 6 primes [51]. In 2012, Tao proved [58] that every odd number $n > 1$ is the sum of at most 5 primes.

There have been other avenues of attack towards the strong conjecture. Using ideas close to those of Vinogradov's, Chudakov [9, 10], Estermann [19] and van der Corput [62] proved (independently from each other) that almost every even number (meaning: all elements of a subset of density 1 in the even numbers) can be written as the sum of two primes. In 1973, J.-

R. Chen showed [4] that every even number n larger than a constant C can be written as the sum of a prime number and the product of at most two primes ($n = p_1+p_2$ or $n = p_1+p_2p_3$). Incidentally, J.-R. Chen himself, together with T.-Z. Wang, was responsible for the best bounds on C (for ternary Goldbach) before Lui and Wang: $C = \exp(\exp(11.503)) < 4 \cdot 10^{43000}$ [6] and $C = \exp(\exp(9.715)) < 6 \cdot 10^{7193}$ [7].

Matters are different if one assumes the Generalized Riemann Hypothesis (GRH). A careful analysis [18] of Hardy and Littlewood's work [23] gives that every odd number $n \geq 1.24 \cdot 10^{50}$ is the sum of three primes if GRH is true. According to [18], the same statement with $n \geq 10^{32}$ was proven in the unpublished doctoral dissertation of B. Lucke, a student of E. Landau's, in 1926. Zinoviev [72] improved this to $n \geq 10^{20}$. A computer check ([16]; see also [55]) showed that the conjecture is true for $n < 10^{20}$, thus completing the proof of the ternary Goldbach conjecture under the assumption of GRH. What was open until now was, of course, the problem of giving an unconditional proof.

2. The circle method: Fourier analysis on $\mathbb{Z}$

It is common for a first course on Fourier analysis to focus on functions over the reals satisfying $f(x) = f(x+1)$, or, what is the same, functions $f : \mathbb{R}/\mathbb{Z} \to \mathbb{C}$. Such a function (unless it is fairly pathological) has a Fourier series converging to it; this is just the same as saying that f has a Fourier transform $\widehat{f} : \mathbb{Z} \to \mathbb{C}$ defined by $\widehat{f}(n) = \int_{\mathbb{R}/\mathbb{Z}} f(\alpha)e(-\alpha n)d\alpha$ and satisfying $f(\alpha) = \sum_{n\in\mathbb{Z}} \widehat{f}(n)e(\alpha n)d\alpha$ (*Fourier inversion theorem*).

In number theory, we are especially interested in functions $f : \mathbb{Z} \to \mathbb{C}$. Then things are exactly the other way around: provided that f decays reasonably fast as $n \to \pm\infty$ (or becomes 0 for n large enough), f has a Fourier transform $\widehat{f} : \mathbb{R}/\mathbb{Z} \to \mathbb{C}$ defined by $\widehat{f}(\alpha) = \sum_n f(n)e(-\alpha n)$ and satisfying $f(n) = \int_{\mathbb{R}/\mathbb{Z}} \widehat{f}(\alpha)e(\alpha n)$. (Highbrow talk: we already knew that $\mathbb{Z}$ is the Fourier dual of $\mathbb{R}/\mathbb{Z}$, and so, of course, $\mathbb{R}/\mathbb{Z}$ is the Fourier dual of $\mathbb{Z}$.) "Exponential sums" (or "trigonometrical sums", as in the title of [69]) are sums of the form $\sum_n f(\alpha)e(-\alpha n)$; the "circle" in "circle method" is just a name for $\mathbb{R}/\mathbb{Z}$.

The study of the Fourier transform $\widehat{f}$ is relevant to additive problems in number theory, i.e., questions on the number of ways of writing n as a sum of k integers of a particular form. Why? One answer could be that $\widehat{f}$ gives us information about the "randomness" of f; if f were the characteristic function of a random set, then $\widehat{f}(\alpha)$ would be very small outside a sharp peak at $\alpha = 0$. We can also give a more concrete and immediate answer. Recall that, in general, the Fourier transform of a convolution equals the product of the transforms; over $\mathbb{Z}$, this means that for the additive convolution

$$(f * g)(n) = \sum_{\substack{m_1,m_2\in\mathbb{Z} \\ m_1+m_2=n}} f(m_1)g(m_2),$$

the Fourier transform satisfies the simple rule

$$\widehat{f * g}(\alpha) = \widehat{f}(\alpha) \cdot \widehat{g}(\alpha).$$

We can see right away from this that $(f * g)(n)$ can be non-zero only if n can be written as $n = m_1 + m_2$ for some m_1, m_2 such that $f(m_1)$ and $g(m_2)$ are non-zero. Similarly,

$(f * g * h)(n)$ can be non-zero only if n can be written as $n = m_1 + m_2 + m_3$ for some m_1, m_2, m_3 such that $f(m_1)$, $f_2(m_2)$ and $f_3(m_3)$ are all non-zero. This suggests that, to study the ternary Goldbach problem, we define $f_1, f_2, f_3 : \mathbb{Z} \to \mathbb{C}$ so that they take non-zero values only at the primes.

Hardy and Littlewood defined $f_1(n) = f_2(n) = f_3(n) = 0$ for n non-prime (and also for $n \leq 0$), and $f_1(n) = f_2(n) = f_3(n) = (\log n)e^{-n/x}$ for n prime (where x is a parameter to be fixed later). Here the factor $e^{-n/x}$ is there to provide "fast decay", so that everything converges; as we will see later, Hardy and Littlewood's choice of $e^{-n/x}$ (rather than some other function of fast decay) comes across in hindsight as being very clever, though not quite best-possible. (Their "choice" was, to some extent, not a choice, but an artifact of their version of the circle method.) The term $\log n$ is there for technical reasons – in essence, it makes sense to put it there because a random integer around n has a chance of about $1/(\log n)$ of being prime.

We can see that $(f_1 * f_2 * f_3)(n) \neq 0$ if and only if n can be written as the sum of three primes. Our task is then to show that $(f_1 * f_2 * f_3)(n)$ (i.e., $(f * f * f)(n)$) is non-zero for every n larger than a constant $C \sim 10^{27}$. Since the transform of a convolution equals a product of transforms,

$$(f_1 * f_2 * f_3)(n) = \int_{\mathbb{R}/\mathbb{Z}} \widehat{f_1 * f_2 * f_3}(\alpha) e(\alpha n) d\alpha = \int_{\mathbb{R}/\mathbb{Z}} (\widehat{f_1}\widehat{f_2}\widehat{f_3})(\alpha) e(\alpha n) d\alpha. \quad (2.1)$$

Our task is thus to show that the integral $\int_{\mathbb{R}/\mathbb{Z}} (\widehat{f_1}\widehat{f_2}\widehat{f_3})(\alpha) e(\alpha n) d\alpha$ is non-zero.

As it happens, $\widehat{f}(\alpha)$ is particularly large when α is close to a rational with small denominator. Moreover, for such α, it turns out we can actually give rather precise estimates for $\widehat{f}(\alpha)$. Define $\mathfrak{M}$ (called the set of *major arcs*) to be a union of narrow arcs around the rationals with small denominator:

$$\mathfrak{M} = \bigcup_{q \leq r} \bigcup_{\substack{a \bmod q \\ (a,q)=1}} \left(\frac{a}{q} - \frac{1}{qQ}, \frac{a}{q} + \frac{1}{qQ}\right),$$

where Q is a constant times x/r, and r will be set later. We can write

$$\int_{\mathbb{R}/\mathbb{Z}} (\widehat{f_1}\widehat{f_2}\widehat{f_3})(\alpha) e(\alpha n) d\alpha = \int_{\mathfrak{M}} (\widehat{f_1}\widehat{f_2}\widehat{f_3})(\alpha) e(\alpha n) d\alpha + \int_{\mathfrak{m}} (\widehat{f_1}\widehat{f_2}\widehat{f_3})(\alpha) e(\alpha n) d\alpha, \quad (2.2)$$

where $\mathfrak{m}$ is the complement $(\mathbb{R}/\mathbb{Z}) \setminus \mathfrak{M}$ (called *minor arcs*).

Now, we simply do not know how to give precise estimates for $\widehat{f}(\alpha)$ when α is in $\mathfrak{m}$. However, as Vinogradov realized, one can give reasonable upper bounds on $|\widehat{f}(\alpha)|$ for $\alpha \in \mathfrak{m}$. This suggests the following strategy: show that

$$\int_{\mathfrak{m}} |\widehat{f_1}(\alpha)||\widehat{f_2}(\alpha)||\widehat{f_3}(\alpha)| d\alpha < \int_{\mathfrak{M}} \widehat{f_1}(\alpha)\widehat{f_2}(\alpha)\widehat{f_3}(\alpha) e(\alpha n) d\alpha. \quad (2.3)$$

By (2.1) and (2.2), this will imply immediately that $(f_1 * f_2 * f_3)(n) > 0$, and so we will be done.

3. The major arcs $\mathfrak{M}$

3.1. What do we really know about L-functions and their zeros? Before we start, let us give a very brief review of basic analytic number theory (in the sense of, say, [13]). A *Dirichlet character* $\chi : \mathbb{Z} \to \mathbb{C}$ of modulus q is a character of $(\mathbb{Z}/q\mathbb{Z})^*$ lifted to $\mathbb{Z}$. (In other words, $\chi(n) = \chi(n+q)$, $\chi(ab) = \chi(a)\chi(b)$ for all a, b and $\chi(n) = 0$ for $(n,q) \neq 1$.) A *Dirichlet L-series* is defined by

$$L(s,\chi) = \sum_{n=1}^{\infty} \chi(n) n^{-s}$$

for $\Re(s) > 1$, and by analytic continuation for $\Re(s) \leq 1$. (The Riemann zeta function $\zeta(s)$ is the L-function for the trivial character, i.e., the character χ such that $\chi(n) = 1$ for all n.) Taking logarithms and then derivatives, we see that

$$-\frac{L'(s,\chi)}{L(s,\chi)} = \sum_{n=1}^{\infty} \Lambda(n) n^{-s}, \tag{3.1}$$

where Λ is the *von Mangoldt function* ($\Lambda(n) = \log p$ if n is some prime power p^α, $\alpha \geq 1$, and $\Lambda(n) = 0$ otherwise).

Dirichlet introduced his characters and L-series so as to study primes in arithmetic progressions. In general, and after some work, (3.1) allows us to restate many sums over the primes (such as our Fourier transforms $\widehat{f}(\alpha)$) as sums over the zeros of $L(s,\chi)$. A *non-trivial zero* of $L(s,\chi)$ is a zero of $L(s,\chi)$ such that $0 < \Re(s) < 1$. (The other zeros are called trivial because we know where they are, namely, at negative integers and, in some cases, also on the line $\Re(s) = 0$. In order to eliminate all zeros on $\Re(s) = 0$ outside $s = 0$, it suffices to assume that χ is *primitive*; a primitive character modulo q is one that is not induced by (i.e., not the restriction of) any character modulo $d|q$, $d < q$.)

The Generalized Riemann Hypothesis for Dirichlet L-functions is the statement that, for every Dirichlet character χ, every non-trivial zero of $L(s,\chi)$ satisfies $\Re(s) = 1/2$. Of course, the Generalized Riemann Hypothesis (GRH) – and the Riemann Hypothesis, which is the special case of χ trivial – remains unproven. Thus, if we want to prove unconditional statements, we need to make do with partial results towards GRH. Two kinds of such results have been proven:

- **Zero-free regions.** Ever since the late nineteenth century (Hadamard, de la Vallée-Poussin) we have known that there are hourglass-shaped regions (more precisely, of the shape $\frac{c}{\log t} \leq \sigma \leq 1 - \frac{c}{\log t}$, where c is a constant and where we write $s = \sigma + it$) outside which non-trivial zeros cannot lie. Explicit values for c are known [35, 36, 42]. There is also the Vinogradov-Korobov region [39, 70], which is broader asymptotically but narrower in most of the practical range (see [20], however).
- **Finite verifications of GRH.** It is possible to (ask the computer to) prove small, finite fragments of GRH, in the sense of verifying that all non-trivial zeros of a given finite set of L-functions with imaginary part less than some constant H lie on the critical line $\Re(s) = 1/2$. Such verifications go back to Riemann, who checked the first few zeros of $\zeta(s)$. Large-scale, rigorous computer-based verifications are now a possibility.

Most work in the literature follows the first alternative, though [58] did use a finite verification of RH (i.e., GRH for the trivial character). Unfortunately, zero-free regions seem

too narrow to be useful for the ternary Goldbach problem. Thus, we are left with the second alternative.

In coordination with the present work, Platt [48] verified that all zeros s of L-functions for characters χ with modulus $q \leq 300000$ satisfying $\Im(s) \leq H_q$ lie on the line $\Re(s) = 1/2$, where

- $H_q = 10^8/q$ for q odd, and
- $H_q = \max(10^8/q, 200 + 7.5 \cdot 10^7/q)$ for q even.

This was a medium-large computation, taking a few hundreds of thousands of core-hours on a parallel computer. It used *interval arithmetic* for the sake of rigor; we will later discuss what this means.

The choice to use a finite verification of GRH, rather than zero-free regions, had consequences on the manner in which the major and minor arcs had to be chosen. As we shall see, such a verification can be used to give very precise bounds on the major arcs, but also forces us to define them so that they are narrow and their number is constant. To be precise: the major arcs were defined around rationals a/q with $q \leq r$, $r = 300000$; moreover, as will become clear, the fact that H_q is finite will force their width to be bounded by $c_0 r/qx$, where c_0 is a constant (say $c_0 = 8$).

3.2. Estimates of $\widehat{f}(\alpha)$ for α in the major arcs. Recall that we want to estimate sums of the type $\widehat{f}(\alpha) = \sum f(n)e(-\alpha n)$, where $f(n)$ is something like $(\log n)\eta(n/x)$ for n equal to a prime, and 0 otherwise; here $\eta : \mathbb{R} \to \mathbb{C}$ is some function of fast decay, such as Hardy and Littlewood's choice, $\eta(t) = e^{-t}$. Let us modify this just a little – we will actually estimate

$$S_\eta(\alpha, x) = \sum \Lambda(n)e(\alpha n)\eta(n/x), \tag{3.2}$$

where Λ is the von Mangoldt function (as in (3.1)) . The use of α rather than $-\alpha$ is just a bow to tradition, as is the use of the letter S (for "sum"); however, the use of $\Lambda(n)$ rather than just plain $\log p$ does actually simplify matters.

The function η here is sometimes called a *smoothing function* or simply a *smoothing*. It will indeed be helpful for it to be smooth on $(0, \infty)$, but, in principle, it need not even be continuous. (Vinogradov's work implicitly uses, in effect, the "brutal truncation" $1_{[0,1]}(t)$, defined to be 1 when $t \in [0, 1]$ and 0 otherwise; that would be fine for the minor arcs, but, as it will become clear, it is a bad idea as far as the major arcs are concerned.)

Assume α is on a major arc, meaning that we can write $\alpha = a/q + \delta/x$ for some a/q (q small) and some δ (with $|\delta|$ small). We can write $S_\eta(\alpha, x)$ as a linear combination

$$S_\eta(\alpha, x) = \sum_\chi c_\chi S_{\eta,\chi}\left(\frac{\delta}{x}, x\right) + \text{tiny error term}, \tag{3.3}$$

where

$$S_{\eta,\chi}\left(\frac{\delta}{x}, x\right) = \sum \Lambda(n)\chi(n)e(\delta n/x)\eta(n/x). \tag{3.4}$$

In (3.3), χ runs over primitive Dirichlet characters of moduli $d|q$, and c_χ is small ($|c_\chi| \leq \sqrt{d}/\phi(q)$).

To estimate the sums $S_{\eta,\chi}$, we will use L-functions, together with one of the most common tools of analytic number theory, the Mellin transform. This transform is essentially a

Laplace transform with a change of variables, and a Laplace transform, in turn, is a Fourier transform taken on a vertical line in the complex plane. For f of fast enough decay, the Mellin transform $F = Mf$ of f is given by

$$F(s) = \int_0^\infty f(t) t^s \frac{dt}{t};$$

we can express f in terms of F by the *Mellin inversion formula*

$$f(t) = \frac{1}{2\pi i} \int_{\sigma - i\infty}^{\sigma + i\infty} F(s) t^{-s} ds$$

for any σ within an interval. We can thus express $e(\delta t)\eta(t)$ in terms of its Mellin transform F_δ and then use (3.1) to express $S_{\eta,\chi}$ in terms of F_δ and $L'(s,\chi)/L(s,\chi)$; shifting the integral in the Mellin inversion formula to the left, we obtain what is known in analytic number theory as an *explicit formula*:

$$S_{\eta,\chi}(\delta/x, x) = [\widehat{\eta}(-\delta)x] - \sum_\rho F_\delta(\rho) x^\rho + \text{tiny error term}.$$

Here the term between brackets appears only for χ trivial. In the sum, ρ goes over all non-trivial zeros of $L(s,\chi)$, and F_δ is the Mellin transform of $e(\delta t)\eta(t)$. (The tiny error term comes from a sum over the trivial zeros of $L(s,\chi)$.) We will obtain the estimate we desire if we manage to show that the sum over ρ is small.

The point is this: if we verify GRH for $L(s,\chi)$ up to imaginary part H, i.e., if we check that all zeroes ρ of $L(s,\chi)$ with $|\Im(\rho)| \le H$ satisfy $\Re(\rho) = 1/2$, we have $|x^\rho| = \sqrt{x}$. In other words, x^ρ is very small (compared to x). However, for any ρ whose imaginary part has absolute value greater than H, we know next to nothing about its real part, other than $0 \le \Re(\rho) \le 1$. (Zero-free regions are notoriously weak for $\Im(\rho)$ large; we will not use them.) Hence, our only chance is to make sure that $F_\delta(\rho)$ is very small when $|\Im(\rho)| \ge H$.

This has to be true for both δ very small (including the case $\delta = 0$) and for δ not so small ($|\delta|$ up to $c_0 r/q$, which can be large because r is a large constant). How can we choose η so that $F_\delta(\rho)$ is very small in both cases for $\tau = \Im(\rho)$ large?

The method of *stationary phase* is useful as an exploratory tool here. In brief, it suggests (and can sometimes prove) that the main contribution to the integral

$$F_\delta(t) = \int_0^\infty e(\delta t)\eta(t) t^s \frac{dt}{t} \tag{3.5}$$

can be found where the phase of the integrand has derivative 0. This happens when $t = -\tau/2\pi\delta$ (for $\operatorname{sgn}(\tau) \ne \operatorname{sgn}(\delta)$); the contribution is then a moderate factor times $\eta(-\tau/2\pi\delta)$. In other words, if $\operatorname{sgn}(\tau) \ne \operatorname{sgn}(\delta)$ and δ is not too small ($|\delta| \ge 8$, say), $F_\delta(\sigma + i\tau)$ behaves like $\eta(-\tau/2\pi\delta)$; if δ is small ($|\delta| < 8$), then F_δ behaves like F_0, which is the Mellin transform $M\eta$ of η. Here is our goal, then: the decay of $\eta(t)$ as $|t| \to \infty$ should be as fast as possible, and the decay of the transform $M\eta(\sigma + i\tau)$ should also be as fast as possible.

This is a classical dilemma, often called the *uncertainty principle* because it is the mathematical fact underlying the physical principle of the same name: you cannot have a function η that decreases extremely rapidly and whose Fourier transform (or, in this case, its Mellin transform) also decays extremely rapidly. What does "extremely rapidly" mean here? It

means (as Hardy himself proved) "faster than any exponential e^{-Ct}". Thus, Hardy and Littlewood's choice $\eta(t) = e^{-t}$ seems essentially optimal at first sight.

However, it is not optimal. We can choose η so that $M\eta$ decreases exponentially (with a constant C somewhat worse than for $\eta(t) = e^{-t}$), but η decreases faster than exponentially. This is a particularly appealing possibility because it is $t/|\delta|$, and not so much t, that risks being fairly small. (To be explicit: say we check GRH for characters of modulus q up to $H_q \sim 50 \cdot c_0 r/q \geq 50|\delta|$. Then we only know that $|\tau/2\pi\delta| \gtrsim 8$. So, for $\eta(t) = e^{-t}$, $\eta(-\tau/2\pi\delta)$ may be as large as e^{-8}, which is not negligible. Indeed, since this term will be multiplied later by other terms, e^{-8} is simply not small enough. On the other hand, we can assume that $H_q \geq 200$ (say), and so $M\eta(s) \sim e^{-(\pi/2)|\tau|}$ is completely negligible, and will remain negligible even if we replace $\pi/2$ by a somewhat smaller constant.)

We shall take $\eta(t) = e^{-t^2/2}$ (that is, the Gaussian). This is not the only possible choice, but it is in some sense natural. It is easy to show that the Mellin transform F_δ for $\eta(t) = e^{-t^2/2}$ is a multiple of what is called a *parabolic cylinder function* $U(a, z)$ with imaginary values for z. There are plenty of estimates on parabolic cylinder functions in the literature – but mostly for a and z real, in part because that is one of the cases occuring most often in applications. There are some asymptotic expansions and estimates for $U(a, z)$, a, z, general, due to Olver (see, e.g., [47]), but unfortunately they come without fully explicit error terms for a and z within our range of interest. (The same holds for [59].)

In the end, using the *saddle-point method*, I derived bounds for the Mellin transform F_δ of $\eta(t)e(\delta t)$ with $\eta(t) = e^{-t^2/2}$: for $s = \sigma + i\tau$ with $\sigma \in [0, 1]$ and $|\tau| \geq \max(100, 4\pi^2|\delta|)$,

$$|F_\delta(s)| + |F_\delta(1-s)| \leq 4.226 \cdot \begin{cases} e^{-0.1065\left(\frac{\tau}{\pi\delta}\right)^2} & \text{if } |\tau| < \frac{3}{2}(\pi\delta)^2, \\ e^{-0.1598|\tau|} & \text{if } |\tau| \geq \frac{3}{2}(\pi\delta)^2. \end{cases} \tag{3.6}$$

Similar bounds hold for σ in other ranges, thus giving us (similar) estimates for the Mellin transform F_δ for $\eta(t) = t^k e^{-t^2/2}$ and σ in the critical range $[0, 1]$.

A moment's thought shows that we can also use (3.6) to deal with the Mellin transform of $\eta(t)e(\delta t)$ for any function of the form $\eta(t) = e^{-t^2/2}g(t)$ (or, more generally, $\eta(t) = t^k e^{-t^2/2}g(t)$), where $g(t)$ is any *band-limited function*. By a band-limited function, we could mean a function whose Fourier transform is compactly supported; while that is a plausible choice, it turns out to be better to work with functions that are band-limited with respect to the Mellin transform – in the sense of being of the form

$$g(t) = \int_{-R}^{R} h(r) t^{-ir} dr,$$

where $h : \mathbb{R} \to \mathbb{C}$ is supported on a compact interval $[-R, R]$, with R not too large (say $R = 200$).

After deriving an explicit formula general enough to work with all the weights $\eta(t)$ we have discussed, and once we consider the input provided by Platt's finite verification of GRH up to H_q, we obtain simple bounds for different weights. For $\eta(t) = e^{-t^2/2}$, $x \geq 10^8$, χ a primitive character of modulus $q \leq r = 300000$, and any $\delta \in \mathbb{R}$ with $|\delta| \leq 4r/q$, we obtain

$$S_{\eta,\chi}\left(\frac{\delta}{x}, x\right) = I_{q=1} \cdot \widehat{\eta}(-\delta)x + E \cdot x, \tag{3.7}$$

where $I_{q=1} = 1$ if $q = 1$, $I_{q=1} = 0$ if $q \neq 1$, and

$$|E| \leq 5.281 \cdot 10^{-22} + \frac{1}{\sqrt{x}} \left(\frac{650400}{\sqrt{q}} + 112 \right). \tag{3.8}$$

Here $\widehat{\eta}$ stands for the Fourier transform from $\mathbb{R}$ to $\mathbb{R}$ normalized as follows:

$$\widehat{\eta}(t) = \int_{-\infty}^{\infty} e(-xt)\eta(x)dx$$

Thus, $\widehat{\eta}(-\delta)$ is just $\sqrt{2\pi}e^{-2\pi^2\delta^2}$ (self-duality of the Gaussian).

This is one of the main results of [27]. Similar bounds are also proven there for $\eta(t) = t^2e^{-t^2/2}$, as well as for a weight of type $\eta(t) = te^{-t^2/2}g(t)$, where $g(t)$ is a band-limited function, and also for a weight η defined by a multiplicative convolution. The conditions on q ($q \leq r = 300000$) and δ are what we expected from the outset.

Thus concludes our treatment of the major arcs. This is arguably the easiest part of the proof; it was actually what I left for the end, as I was fairly confident it would work out.

4. The minor arcs $\mathfrak{m}$

4.1. Qualitative goals and main ideas. What kind of bounds do we need? What is there in the literature?

We wish to obtain upper bounds on $|S_\eta(\alpha, x)|$ for some weight η and any $\alpha \in \mathbb{R}/\mathbb{Z}$ not very close to a rational with small denominator. Every α is close to some rational a/q; what we are looking for is a bound on $|S_\eta(\alpha, x)|$ that decreases rapidly when q increases.

Moreover, we want our bound to decrease rapidly when δ increases, where $\alpha = a/q + \delta/x$. In fact, the main terms in our bound will be decreasing functions of $\max(1, |\delta|/8) \cdot q$. (Let us write $\delta_0 = \max(2, |\delta|/4)$ from now on.) This will allow our bound to be good enough outside narrow major arcs, which will get narrower and narrower as q increases – that is, precisely the kind of major arcs we were presupposing in our major-arc bounds.

It would be possible to work with narrow major arcs that become narrower as q increases simply by allowing q to be very large (close to x), and assigning each angle to the fraction closest to it. This is the common procedure. However, this makes matters more difficult, in that we would have to minimize at the same time the factors in front of terms x/q, $x/\sqrt{q}$, etc., and those in front of terms q, $\sqrt{qx}$, and so on. (These terms are being compared to the trivial bound x.) Instead, we choose to strive for a direct dependence on δ throughout; this will allow us to cap q at a much lower level, thus making terms such as q and $\sqrt{qx}$ negligible.

How good must our bounds be? Since the major-arc bounds are valid only for $q \leq r = 300000$ and $|\delta| \leq 4r/q$, we cannot afford even a single factor of $\log x$ (or any other function tending to ∞ as $x \to \infty$) in front of terms such as $x/\sqrt{q|\delta_0|}$: a factor like that would make the term larger than the trivial bound x for $q|\delta_0|$ equal to a constant (r, say) and x very large. Apparently, there was no such "log-free bound" with explicit constants in the literature, even though such bounds were considered to be in principle feasible, and even though previous work ([5, 11, 12, 58]) had gradually decreased the number of factors of $\log x$. (In limited ranges for q, there were log-free bounds without explicit constants; see [11, 53]. The estimate in [69, Thm. 2a, 2b] was almost log-free, but not quite. There were

also bounds [3, 37] that used L-functions, and thus were not really useful in a truly minor-arc regime.)

It also seemed clear that a main bound proportional to $(\log q)^2 x/\sqrt{q}$ (as in [58]) was too large. At the same time, it was not really necessary to reach a bound of the best possible form that could be found through Vinogradov's basic approach, namely

$$|S_\eta(\alpha, x)| \leq C\frac{x\sqrt{q}}{\phi(q)}. \tag{4.1}$$

Such a bound had been proven by Ramaré [53] for q in a limited range and C non-explicit; later, in [50] Ramaré broadened the range to $q \leq x^{1/48}$ and gave an explicit value for C, namely, $C = 13000$. Such a bound is a notable achievement, but, unfortunately, it is not useful for our purposes. Rather, we will aim at a bound whose main term is bounded by a constant around 1 times $x(\log \delta_0 q)/\sqrt{\delta_0 \phi(q)}$; this is slightly worse asymptotically than (4.1), but it is much better in the delicate range of $\delta_0 q \sim 300000$.

* * *

We see that we have several tasks. One of them is the removal of logarithms: we cannot afford a single factor of $\log x$, and, in practice, we can afford at most one factor of $\log q$. Removing logarithms will be possible in part because of the use of efficient techniques (the large sieve for sequences with prime support) but also because we will be able to find cancellation at several places in sums coming from a combinatorial identity (namely, Vaughan's identity). The task of finding cancellation efficiently (that is, with good constants) is particularly delicate. Bounding a sum such as $\sum_n \mu(n)$ efficiently is harder than estimating a sum such as $\sum_n \Lambda(n)$ equally well, even though we are used to thinking of these problems as equivalent.

We have said that our bounds will improve as $|\delta|$ increases. This dependence on δ will be secured in different ways at different places. Sometimes δ will appear as an argument, as in $\widehat{\eta}(-\delta)$; for η piecewise continuous with $\eta' \in L_1$, we know that $|\widehat{\eta}(t)| \to 0$ as $|t| \to \infty$. Sometimes we will obtain a dependence on δ by using several different rational approximations to the same $\alpha \in \mathbb{R}$. Lastly, we will obtain a good dependence on δ in bilinear sums by supplying a scattered input to a large sieve.

If there is a main moral to the argument, it lies in the close relation between the circle method and the large sieve. The circle method rests on the estimation of an integral involving a Fourier transform $\widehat{f} : \mathbb{R}/\mathbb{Z} \to \mathbb{C}$; as we will later see, this leads naturally to estimating the ℓ_2-norm of $\widehat{f}$ on subsets (namely, unions of arcs) of the circle $\mathbb{R}/\mathbb{Z}$. The large sieve can be seen as an approximate discrete version of Plancherel's identity, which states that $|\widehat{f}|_2 = |f|_2$.

Both in this section and in §5, we shall use the large sieve in part so as to use the fact that some of the functions we work with have prime support, i.e., are non-zero only on prime numbers. There are ways to use prime support to improve the output of the large sieve. In §5, these techniques will be refined and then translated to the context of the circle method, where f has (essentially) prime support and $|\widehat{f}|^2$ must be integrated over unions of arcs. The main point is that the large sieve is not being used as a black box; rather, we can adapt ideas from (say) the large-sieve context and apply them to the circle method.

Lastly, there are the benefits of a continuous η. Hardy and Littlewood already used a continuous η; this was abandoned by Vinogradov, presumably for the sake of simplicity.

The idea that smooth weights η can be superior to sharp truncations is now commonplace. As we shall see, using a continuous η is helpful in the minor-arcs regime, but not as crucial there as for the major arcs. We will not use a smooth η; we will prove our estimates for any continuous η that is piecewise C_1, and then, towards the end, we will choose to use the same weight $\eta = \eta_2$ as in [58], in part because it has compact support, and in part for the sake of comparison. The moral here is not quite the common dictum "always smooth", but rather that different kinds of smoothing can be appropriate for different tasks; in the end, we will show how to coordinate different smoothing functions η.

4.2. Combinatorial identities. Generally, since Vinogradov, a treatment of the minor arcs starts with a combinatorial identity expressing $\Lambda(n)$ (or the characteristic function of the primes) as a sum of two or more convolutions. (In this section, by a convolution $f * g$, we will mean the *Dirichlet convolution* $(f * g)(n) = \sum_{d|n} f(d)g(n/d)$, i.e., the multiplicative convolution on the semigroup of positive integers.)

In some sense, the archetypical identity is

$$\Lambda = \mu * \log,$$

but it will not usually do: the contribution of $\mu(d)\log(n/d)$ with d close to n is too difficult to estimate precisely. There are alternatives: for example, there is Selberg's identity

$$\Lambda(n)\log n = \mu * \log^2 - \Lambda * \Lambda, \tag{4.2}$$

or the generalization of this to $\Lambda(n)(\log n)^k = \mu * \log^{k+1} - \dots$ (Bomberi-Selberg). Another useful (and very simple) identity was that used by Daboussi's [12].

The proof of Vinogradov's three-prime result was simplified substantially in [64] by the introduction of *Vaughan's identity*:

$$\Lambda(n) = \mu_{\le U} * \log - \Lambda_{\le V} * \mu_{\le U} * 1 + 1 * \mu_{>U} * \Lambda_{>V} + \Lambda_{\le V}, \tag{4.3}$$

where we are using the notation

$$f_{\le W} = \begin{cases} f(n) & \text{if } n \le W, \\ 0 & \text{if } n > W, \end{cases} \qquad f_{>W} = \begin{cases} 0 & \text{if } n \le W, \\ f(n) & \text{if } n > W. \end{cases}$$

Of the resulting sums ($\sum_n (\mu_{\le U} * \log)(n) e(\alpha n)\eta(n/x)$, etc.), the first three are said to be of *type I*, *type I* (again) and *type II*; the last sum, $\sum_{n \le V} \Lambda(n)$, is negligible.

One of the advantages of Vaughan's identity is its flexibility: we can set U and V to whatever values we wish. Its main disadvantage is that it is not "log-free", in that it seems to impose the loss of two factors of $\log x$: if we sum each side of (4.3) from 1 to x, we obtain $\sum_{n \le x} \Lambda(n) \sim x$ on the left side, whereas, if we bound the sum on the right side without the use of cancellation, we obtain a bound of $x(\log x)^2$. Of course, we will obtain some cancellation from the phase $e(\alpha n)$, but that is not enough.

As was pointed out in [58], it is possible to get a factor of $(\log q)^2$ instead of a factor of $(\log x)^2$ in the type II sums by setting U and V appropriately. A factor of $(\log q)^2$ is still too large in practice, and there are also the factors of $\log x$ in type I sums. Vinogradov had already managed to get an essentially log-free result (by a rather difficult procedure) in [69, Ch. IX]. The result in [11] is log-free. Unfortunately, the explicit result in [12] – the study of which encouraged me at the beginning of the project – is not. For a while, I worked with

the Bombieri-Selberg identity with $k = 2$. Ramaré obtained a log-free bound in [53] using the Diamond-Steinig identity, which is related to Bombieri-Selberg.

In the end, I decided to use Vaughan's identity. This posed a challenge: to obtain cancellation in Vaughan's identity at every possible step, beyond the cancellation given by the phase $e(\alpha n)$. It is clear that the presence of the Möbius function μ should give, in principle, some cancellation; we will show how to use it to obtain as much cancellation as we need.

4.3. Type I sums. There are two type I sums, namely,

$$\sum_{m\le U} \mu(m) \sum_n (\log n) e(\alpha m n) \eta\left(\frac{mn}{x}\right) \tag{4.4}$$

and

$$\sum_{v\le V} \Lambda(v) \sum_{u\le U} \mu(u) \sum_n e(\alpha v u n) \eta\left(\frac{vun}{x}\right). \tag{4.5}$$

In either case, $\alpha = a/q + \delta/x$, where q is larger than a constant r and $|\delta/x| \le 1/qQ_0$ for some $Q_0 > \max(q, \sqrt{x})$. For the purposes of this exposition, we will set it as our task to estimate the slightly simpler sum

$$\sum_{m\le D} \mu(m) \sum_n e(\alpha m n) \eta\left(\frac{mn}{x}\right), \tag{4.6}$$

where D can be U or UV or something else less than x.

Why can we consider this simpler sum without omitting anything essential? It is clear that (4.4) is of the same kind as (4.6). The inner double sum in (4.5) is just (4.6) with αv instead of α; this enables us to estimate (4.5) by means of (4.6) for q small, i.e., the more delicate case. If q is not small, then the approximation $\alpha v \sim av/q$ may not be accurate enough. In that case, we collapse the two outer sums in (4.5) into a sum $\sum_n (\Lambda_{\le V} * \mu_{\le U})(n)$, and treat all of (4.5) much as we will treat (4.6); since q is not small, we can afford to bound $(\Lambda_{\le V} * \mu_{\le U})(n)$ trivially (by $\log n$) in the less sensitive terms.

Let us first outline Vinogradov's procedure for bounding type I sums. Just by summing a geometric series, we get $\left|\sum_{n\le N} e(\alpha n)\right| \le \min(N, c/\{\alpha\})$, where c is a constant and $\{\alpha\}$ is the distance from α to the nearest integer. Vinogradov splits the outer sum in (4.6) into sums of length q. When m runs on an interval of length q, the angle am/q runs through all fractions of the form b/q; due to the error δ/x, αm could be close to 0 for two values of n, but otherwise $\{\alpha m\}$ takes values bounded below by $1/q$, $2/q$, etc. Thus

$$\left|\sum_{y<m\le y+q} \mu(m) \sum_{n\le N} e(\alpha m n)\right| \le \sum_{y<m\le y+q} \left|\sum_{n\le N} e(\alpha m n)\right| \le \frac{2N}{m} + 2cq \log eq \tag{4.7}$$

for any $y \ge 0$.

There are several ways to improve this. One is simply to estimate the inner sum more precisely; this was already done in [12]. One can also define a smoothing function η, as in (4.6); it is easy to get

$$\left|\sum_{n\le N} e(\alpha n) \eta\left(\frac{n}{x}\right)\right| \le \min\left(x|\eta|_1 + \frac{|\eta'|_1}{2}, \frac{|\eta'|_1}{2|\sin(\pi\alpha)|}, \frac{|\widehat{\eta''}|_\infty}{4x(\sin \pi\alpha)^2}\right).$$

Except for the third term, this is as in [58]. We could also choose carefully which bound to use for each m; surprisingly, this gives an improvement – in fact, an important one, for m large. However, we still get a term proportional to N/m as in (4.7), and this contributes about $(x \log x)/q$ to the sum (4.6), thus giving us an estimate that is not log-free.

What we have to do, naturally, is to take out the terms with $q|m$ for m small. We obtain a log-free bound for the sum over the terms with $m \le M = \min(D, Q/2)$ with $q \nmid m$, since αm is then never too close to 0. For $m \le M$ divisible by q, we can estimate the inner sum in (4.6) by the Poisson summation formula; writing $m = aq$, we get a main term

$$\frac{x\mu(q)}{q} \cdot \widehat{\eta}(-\delta) \cdot \sum_{\substack{a \le M/q \\ (a,q)=1}} \frac{\mu(a)}{a}, \tag{4.8}$$

where (a, q) stands for the greatest common divisor of a and q. It is clear that we have to get cancellation over μ here. There is an elegant elementary argument [22] showing that the absolute value of the sum in (4.8) is at most 1. We need to gain one more log, however. This was done by Ramaré [49].

What shall we do for $m > Q/2$? We can always give a bound

$$\sum_{y < m \le y+q} \min\left(A, \frac{C}{|\sin \pi\alpha n|^2}\right) \le 3A + \frac{4q}{\pi}\sqrt{AC} \tag{4.9}$$

for y arbitrary; since AC will be of constant size, $(4q/\pi)\sqrt{AC}$ is pleasant enough, but the contribution of $3A \sim 3|\eta|_1 x/y$ seems lethal (it adds a multiple of $(x \log x)/q$ to the total) and at first sight unavoidable: the values of m for which αm is close to 0 no longer correspond to the congruence class $m \equiv 0 \bmod q$, and thus cannot be taken out.

The solution is to switch approximations. (The idea of using different approximations to the same α is neither new nor recent in the general context of the circle method: see [66, §2.8, Ex. 2]. What may be new is its use to clear a hurdle in type I sums.) What does this mean? If α were exactly, or almost exactly, a/q, then there would be no other very good approximations in a reasonable range. However, note that we can *define* $Q = \lfloor x/|\delta q| \rfloor$ for $\alpha = a/q + \delta/x$, and still have $|\alpha - a/q| \le 1/qQ$. If δ is very small, Q will be larger than $2D$, and there will be no terms with $Q/2 < m \le D$ to worry about.

What happens if δ is not very small? We know that, for any Q', there is an approximation a'/q' to α with $|\alpha - a'/q'| \le 1/q'Q'$ and $q' \le Q'$. However, for $Q' > Q$, we know that a'/q' cannot equal a/q: by the definition of Q, the approximation a/q is not good enough, i.e., $|\alpha - a/q| \le 1/qQ'$ does not hold. Since $a/q \ne a'/q'$, we see that $|a/q - a'/q'| \ge 1/qq'$, and, if we take $Q' \ge (1+\epsilon)Q$, this implies that q' is relatively large ($q' \ge (\epsilon/(1+\epsilon))Q$).

Thus, for $m > Q/2$, the solution is to apply (4.9) with a'/q' instead of a/q. The contribution of A fades into insignificance: for the first sum over a range $y < m \le y + q'$, $y \ge Q/2$, it contributes at most $x/(Q/2)$, and all the other contributions of A sum up to at most a constant times $(x \log x)/q'$.

Proceeding in this way, we obtain a total bound for (4.6) whose main terms are proportional to

$$\frac{1}{\phi(q)} \frac{x}{\log \frac{x}{q}} \min\left(1, \frac{1}{\delta^2}\right), \quad \frac{2}{\pi}\sqrt{|\widehat{\eta''}|_\infty} \cdot D \quad \text{and} \quad q \log \max\left(\frac{D}{q}, q\right), \tag{4.10}$$

with good, explicit constants. The first term – usually the largest one – is precisely what we needed: it is proportional to $(1/\phi(q))x/\log x$ for q small, and decreases rapidly as $|\delta|$ increases.

4.4. Type II, or bilinear, sums. We must now bound

$$S = \sum_m (1 * \mu_{>U})(m) \sum_{n>V} \Lambda(n) e(\alpha mn) \eta(mn/x).$$

At this point it is convenient to assume that η is the Mellin convolution of two functions. The *multiplicative* or *Mellin convolution* on $\mathbb{R}^+$ is defined by

$$(\eta_0 *_M \eta_1)(t) = \int_0^\infty \eta_0(r)\eta_1\left(\frac{t}{r}\right)\frac{dr}{r}.$$

Tao [58] takes $\eta = \eta_2 = \eta_1 *_M \eta_1$, where η_1 is a brutal truncation, viz., the function taking the value 2 on $[1/2, 1]$ and 0 elsewhere. We take the same η_2, in part for comparison purposes, and in part because this will allow us to use off-the-shelf estimates on the large sieve. (Brutal truncations are rarely optimal in principle, but, as they are very common, results for them have been carefully optimized in the literature.) Clearly

$$S = \int_V^{X/U} \sum_m \left(\sum_{\substack{d>U\\ d|m}} \mu(d)\right) \eta_1\left(\frac{m}{x/W}\right) \cdot \sum_{n\geq V} \Lambda(n) e(\alpha mn) \eta_1\left(\frac{n}{W}\right)\frac{dW}{W}. \tag{4.11}$$

By Cauchy-Schwarz, the integrand is at most $\sqrt{S_1(U,W)S_2(V,W)}$, where

$$\begin{aligned} S_1(U,W) &= \sum_{\frac{x}{2W} < m \leq \frac{x}{W}} \left|\sum_{\substack{d>U\\ d|m}} \mu(d)\right|^2, \\ S_2(V,W) &= \sum_{\frac{x}{2W} \leq m \leq \frac{x}{W}} \left|\sum_{\max\left(V, \frac{W}{2}\right) \leq n \leq W} \Lambda(n) e(\alpha mn)\right|^2. \end{aligned} \tag{4.12}$$

We must bound $S_1(U,W)$ by a constant times x/W. We are able to do this – with a good constant. (A careless bound would have given a multiple of $(x/U)\log^3(x/U)$, which is much too large.) First, we reduce $S_1(U,W)$ to an expression involving an integral of

$$\sum_{\substack{r_1\leq x\\ (r_1,r_2)=1}} \sum_{r_2\leq x} \frac{\mu(r_1)\mu(r_2)}{\sigma(r_1)\sigma(r_2)}. \tag{4.13}$$

We can bound (4.13) by the use of bounds on $\sum_{n\leq t}\mu(n)/n$, combined with the estimation of infinite products by means of approximations to $\zeta(s)$ for $s \to 1^+$. After some additional manipulations, we obtain a bound for $S_1(U,W)$ whose main term is at most $(3/\pi^2)(x/W)$ for each W, and closer to $0.22482x/W$ on average over W.

(This is as good a point as any to say that, throughout, we can use a trick in [58] that allows us to work with odd values of integer variables throughout, instead of letting m or n range over all integers. Here, for instance, if m and n are restricted to be odd, we obtain a bound of $(2/\pi^2)(x/W)$ for individual W, and $0.15107x/W$ on average over W.)

Let us now bound $S_2(V, W)$. This is traditionally done by Linnik's dispersion method. However, it should be clear that the thing to do nowadays is to use a large sieve, and, more specifically, a large sieve for primes. In order to take advantage of prime support, we use Montgomery's inequality ([33, 43]; see the expositions in [44, pp. 27–29] and [34, §7.4]) combined with Montgomery and Vaughan's large sieve with weights [45, (1.6)], following the general procedure in [45, (1.6)]. We obtain a bound of the form

$$\frac{\log W}{\log \frac{W}{2q}} \left(\frac{x}{4\phi(q)} + \frac{qW}{\phi(q)} \right) \frac{W}{2} \tag{4.14}$$

on $S_2(V, W)$, where, of course, we can also choose *not* to gain a factor of $\log W/2q$ if q is close to or greater than W.

It remains to see how to gain a factor of $|\delta|$ in the major arcs, and more specifically in $S_2(V, W)$. To explain this, let us step back and take a look at what the large sieve is. Given a civilized function $f : \mathbb{Z} \to \mathbb{C}$, Plancherel's identity tells us that

$$\int_{\mathbb{R}/\mathbb{Z}} \left| \widehat{f}\,(\alpha) \right|^2 d\alpha = \sum_n |f(n)|^2.$$

The large sieve can be seen as an approximate, or statistical, version of this: for a "sample" of points $\alpha_1, \alpha_2, \dots, \alpha_k$ satisfying $|\alpha_i - \alpha_j| \geq \beta$ for $i \neq j$, it tells us that

$$\sum_{1 \leq j \leq k} \left| \widehat{f}\,(\alpha_j) \right|^2 \leq (X + \beta^{-1}) \sum_n |f(n)|^2, \tag{4.15}$$

assuming that f is supported on an interval of length X.

Now consider $\alpha_1 = \alpha, \alpha_2 = 2\alpha, \alpha_3 = 3\alpha \dots$. If $\alpha = a/q$, then the angles $\alpha_1, \dots, \alpha_q$ are well-separated, i.e., they satisfy $|\alpha_i - \alpha_j| \geq 1/q$, and so we can apply (4.15) with $\beta = 1/q$. However, $\alpha_{q+1} = \alpha_1$. Thus, if we have an outer sum of length $L > q$ – in (4.12), we have an outer sum of length $L = x/2W$ – we need to split it into $\lceil L/q \rceil$ blocks of length q, and so the total bound given by (4.15) is $\lceil L/q \rceil (X + q) \sum_n |f(n)|^2$. Indeed, this is what gives us (4.14), which is fine, but we want to do better for $|\delta|$ larger than a constant.

Suppose, then, that $\alpha = a/q + \delta/x$, where $|\delta| > 8$, say. Then the angles α_1 and α_{q+1} are not identical: $|\alpha_1 - \alpha_{q+1}| \leq q|\delta|/x$. We also see that α_{q+1} is at a distance at least $q|\delta|/x$ from $\alpha_2, \alpha_3, \dots \alpha_q$, provided that $q|\delta|/x < 1/q$. We can go on with $\alpha_{q+2}, \alpha_{q+3}, \dots$, and stop only once there is overlap, i.e., only once we reach α_m such that $m|\delta|/x \geq 1/q$. We then give all the angles $\alpha_1, \dots, \alpha_m$ – which are separated by at least $q|\delta|/x$ from each other – to the large sieve at the same time. We do this $\lceil L/m \rceil \leq \lceil L/(x/|\delta|q) \rceil$ times, and obtain a total bound of $\lceil L/(x/|\delta|q) \rceil (X + x/|\delta|q) \sum_n |f(n)|^2$, which, for $L = x/2W$, $X = W/2$, gives us about

$$\left(\frac{x}{4Q} \frac{W}{2} + \frac{x}{4} \right) \log W$$

provided that $L \geq x/|\delta|q$ and, as usual, $|\alpha - a/q| \leq 1/qQ$. This is very small compared to the trivial bound $\lesssim xW/8$.

What happens if $L < x/|\delta q|$? Then there is never any overlap: we consider all angles α_i, and give them all together to the large sieve. The total bound is $(W^2/4 + xW/2|\delta|q) \log W$. If $L = x/2W$ is smaller than, say, $x/3|\delta q|$, then we see clearly that there are non-intersecting swarms of α_i around the rationals a/q. We can thus save a factor of $\log$ (or rather $(\phi(q)/q) \log (W/|\delta q|)$) by applying Montgomery's inequality, which operates by strewing displacements of the given angles (or, here, the swarms) around the circle to the extent possible while keeping everything well-separated. In this way, we obtain a bound of the form

$$\frac{\log W}{\log \frac{W}{|\delta|q}} \left(\frac{x}{|\delta|\phi(q)} + \frac{q}{\phi(q)} \frac{W}{2} \right) \frac{W}{2}.$$

Compare this to (4.14); we have gained a factor of $|\delta|/4$, and so we use this estimate when $|\delta| > 4$. (In [28], the criterion is $|\delta| > 8$, but, since there we have $2\alpha = a/q + \delta/x$, the value of δ there is twice what it is here; this is a consequence of working with sums over the odd integers, as in [58].)

* * *

We have succeeded in eliminating all factors of $\log$ we came across. The only factor of $\log$ that remains is $\log x/UV$, coming from the integral $\int_V^{x/U} dW/W$. Thus, we want UV to be close to x, but we cannot let it be too close, since we also have a term proportional to $D = UV$ in (4.10), and we need to keep it substantially smaller than x. We set U and V so that UV is $x/\sqrt{q \max(4, |\delta|)}$ or thereabouts.

In the end, after some work, we obtain the main result in [28]. We recall that $S_\eta(\alpha, x) = \sum_n \Lambda(n) e(\alpha n) \eta(n/x)$ and $\eta_2 = \eta_1 *_M \eta_1 = 4 \cdot 1_{[1/2,1]} * 1_{[1/2,1]}$.

Theorem 4.1. *Let $x \geq x_0$, $x_0 = 2.16 \cdot 10^{20}$. Let $2\alpha = a/q + \delta/x$, $q \leq Q$, $\gcd(a, q) = 1$, $|\delta/x| \leq 1/qQ$, where $Q = (3/4)x^{2/3}$. If $q \leq x^{1/3}/6$, then*

$$|S_\eta(\alpha, x)| \leq \frac{R_{x,\delta_0 q} \log \delta_0 q + 0.5}{\sqrt{\delta_0 \phi(q)}} \cdot x + \frac{2.5x}{\sqrt{\delta_0 q}} + \frac{2x}{\delta_0 q} \cdot L_{x,\delta_0,q} + 3.2x^{5/6}, \tag{4.16}$$

where $\delta_0 = \max(2, |\delta|/4)$,

$$\begin{aligned} R_{x,t} &= 0.27125 \log \left(1 + \frac{\log 4t}{2 \log \frac{9x^{1/3}}{2.004t}} \right) + 0.41415 \\ L_{x,\delta,q} &= \frac{\log \delta^{\frac{7}{4}} q^{\frac{13}{4}} + \frac{80}{9}}{\phi(q)/q} + \log q^{\frac{80}{9}} \delta^{\frac{16}{9}} + \frac{111}{5}. \end{aligned} \tag{4.17}$$

If $q > x^{1/3}/6$, then

$$|S_\eta(\alpha, x)| \leq 0.2727 x^{5/6} (\log x)^{3/2} + 1218 x^{2/3} \log x.$$

The factor $R_{x,t}$ is small in practice; for typical "difficult" values of x and $\delta_0 x$, it is less than 1. The crucial things to notice in (4.16) are that there is no factor of $\log x$, and that, in the main term, there is only one factor of $\log \delta_0 q$. The fact that δ_0 helps us as it grows is precisely what enables us to take major arcs that get narrower and narrower as q grows.

5. Integrals over the major and minor arcs

So far, we have sketched (§3) how to estimate $S_\eta(\alpha, x)$ for α in the major arcs and η based on the Gaussian $e^{-t^2/2}$, and also (§4) how to bound $|S_\eta(\alpha, x)|$ for α in the minor arcs and $\eta = \eta_2$, where $\eta_2 = 4 \cdot 1_{[1/2,1]} *_M 1_{[1/2,1]}$. We now must show how to use such information to estimate integrals such as the ones in (2.3).

We will use two smoothing functions η_+, η_*; in the notation of (2.2), we set $f_1 = f_2 = \Lambda(n)\eta_+(n/x)$, $f_3 = \Lambda(n)\eta_*(n/x)$, and so we must give a lower bound for

$$\int_{\mathfrak{M}} (S_{\eta_+}(\alpha, x))^2 S_{\eta_*}(\alpha, x) e(-\alpha n) d\alpha \tag{5.1}$$

and an upper bound for

$$\int_{\mathfrak{m}} \left|S_{\eta_+}(\alpha, x)\right|^2 S_{\eta_*}(\alpha, x) e(-\alpha n) d\alpha \tag{5.2}$$

so that we can verify (2.3).

The traditional approach to (5.2) is to bound

$$\begin{aligned} \int_{\mathfrak{m}} (S_{\eta_+}(\alpha, x))^2 S_{\eta_*}(\alpha, x) e(-\alpha n) d\alpha &\le \int_{\mathfrak{m}} \left|S_{\eta_+}(\alpha, x)\right|^2 d\alpha \cdot \max_{\alpha \in \mathfrak{m}} \widehat{\eta_*}(\alpha) \\ &\le \sum_n \Lambda(n)^2 \eta_+^2\left(\frac{n}{x}\right) \cdot \max_{\alpha \in \mathfrak{m}} S_{\eta_*}(\alpha, x). \end{aligned} \tag{5.3}$$

Since the sum over n is of the order of $x \log x$, this is not log-free, and so cannot be good enough; we will later see how to do better. Still, this gets the main shape right: our bound on (5.2) will be proportional to $|\eta_+|_2^2 |\eta_*|_1$. Moreover, we see that η_* has to be such that we know how to bound $|S_{\eta_*}(\alpha, x)|$ for $\alpha \in \mathfrak{m}$, while our choice of η_+ is more or less free, at least as far as the minor arcs are concerned.

What about the major arcs? In order to do anything on them, we will have to be able to estimate both $\eta_+(\alpha)$ and $\eta_*(\alpha)$ for $\alpha \in \mathfrak{M}$. Once we do this, we will obtain that the main term of (5.1) is an infinite product (independent of the smoothing functions), times x^2, times

$$\int_0^\infty \int_0^\infty \eta_+(t_1)\eta_+(t_2)\eta_*\left(\frac{n}{x} - (t_1 + t_2)\right) dt_1 dt_2. \tag{5.4}$$

In other words, we want to maximize (or nearly maximize) the expression on the right of (5.4) divided by $|\eta_+|_2^2 |\eta_*|_1$.

One way to do this is to let η_* be concentrated on a small interval $[0, \epsilon)$. Then the right side of (5.4) is approximately

$$|\eta_*|_1 \cdot \int_0^\infty \eta_+(t)\eta_+\left(\frac{n}{x} - t\right) dt. \tag{5.5}$$

To maximize this, we should make sure that $\eta_+(t) \sim \eta_+(n/x - t)$. We set $x \sim n/2$, and see that we should define η_+ so that it is supported on $[0, 2]$ and symmetric around $t = 1$, or nearly so; this will maximize the ratio of (5.5) to $|\eta_+|_2^2 |\eta_*|_1$.

We should do this while making sure that we will know how to estimate $S_{\eta_+}(\alpha, x)$ for $\alpha \in \mathfrak{M}$. We know how to estimate $S_\eta(\alpha, x)$ very precisely for functions of the form

$\eta(t) = g(t)e^{-t^2/2}$, $\eta(t) = g(t)te^{-t^2/2}$, etc., where $g(t)$ is band-limited. We will work with a function η_+ of that form, chosen so as to be very close (in ℓ_2 norm) to a function $\eta_\circ$ that is in fact supported on $[0, 2]$ and symmetric around $t = 1$.

We choose

$$\eta_\circ(t) = \begin{cases} t^2(2-t)^3 e^{-(t-1)^2/2} & \text{if } t \in [0,2], \\ 0 & \text{if } t \notin [0,2]. \end{cases}$$

This function is obviously symmetric ($\eta_\circ(t) = \eta_\circ(2-t)$) and vanishes to high order at $t = 0$, besides being supported on $[0, 2]$.

We set $\eta_+(t) = h_R(t)te^{-t^2/2}$, where $h_R(t)$ is an approximation to the function

$$h(t) = \begin{cases} t^2(2-t)^3 e^{t-\frac{1}{2}} & \text{if } t \in [0,2] \\ 0 & \text{if } t \notin [0,2]. \end{cases}$$

We just let $h_R(t)$ be the inverse Mellin transform of the truncation of Mh to an interval $[-iR, iR]$, or, what is the same,

$$h_R(t) = \int_0^\infty h(ty^{-1}) F_R(y) \frac{dy}{y},$$

where $F_R(t) = \sin(R \log y)/(\pi \log y)$ (the Dirichlet kernel with a change of variables); since the Mellin transform of $te^{-t^2/2}$ is regular at $s = 0$, the Mellin transform $M\eta_+$ will be holomorphic in a neighborhood of $\{s : 0 \le \Re(s) \le 1\}$, even though the truncation of Mh to $[-iR, iR]$ is brutal. Set $R = 200$, say. By the fast decay of $Mh(it)$ and the fact that the Mellin transform M is an isometry, $|(h_R(t) - h(t))/t|_2$ is very small, and hence so is $|\eta_+ - \eta_\circ|_2$, as we desired.

But what about the requirement that we be able to estimate $S_{\eta_*}(\alpha, x)$ for both $\alpha \in \mathfrak{m}$ and $\alpha \in \mathfrak{M}$?

Generally speaking, if we know how to estimate $S_{\eta_1}(\alpha, x)$ for some $\alpha \in \mathbb{R}/\mathbb{Z}$ and we also know how to estimate $S_{\eta_2}(\alpha, x)$ for all other $\alpha \in \mathbb{R}/\mathbb{Z}$, where η_1 and η_2 are two smoothing functions, then we know how to estimate $S_{\eta_3}(\alpha, x)$ for all $\alpha \in \mathbb{R}/\mathbb{Z}$, where $\eta_3 = \eta_1 *_M \eta_2$, or, more generally, $\eta_*(t) = (\eta_1 *_M \eta_2)(\kappa t)$, $\kappa > 0$ a constant. This is a simple exercise in exchanging the order of integration and summation:

$$\begin{aligned} S_{\eta_*}(\alpha, x) &= \sum_n \Lambda(n) e(\alpha n) (\eta_1 *_M \eta_2)\left(\kappa \frac{n}{x}\right) \\ &= \int_0^\infty \sum_n \Lambda(n) e(\alpha n) \eta_1(\kappa r) \eta_2\left(\frac{n}{rx}\right) \frac{dr}{r} = \int_0^\infty \eta_1(\kappa r) S_{\eta_2}(rx) \frac{dr}{r}, \end{aligned}$$

and similarly with η_1 and η_2 switched.

Now that we have chosen our smoothing weights η_+ and η_*, we have to estimate the major-arc integral (5.1) and the minor-arc integral (5.2). What follows can actually be done for general η_+ and η_*; we could have left our particular choice of η_+ and η_* for the end.

Estimating the major-arc integral (5.1) may sound like an easy task, since we have rather precise estimates for $S_\eta(\alpha, x)$ ($\eta = \eta_+, \eta_*$) when α is on the major arcs; we could just replace $S_\eta(\alpha, x)$ in (5.1) by the approximation given by (3.3) and (3.7). It is, however, more efficient to express (5.1) as the sum of the contribution of the trivial character (a sum of

integrals of $(\widehat{\eta}(-\delta)x)^3$, where $\widehat{\eta}(-\delta)x$ comes from (3.7)), plus a term of the form

$$(\text{maximum of } \sqrt{q}\cdot E(q) \text{ for } q\le r)\cdot \int_{\mathfrak{M}} \left|S_{\eta_+}(\alpha,x)\right|^2 d\alpha,$$

where $E(q)=E$ is as in (3.8), plus two other terms of the same form. As usual, the major arcs $\mathfrak{M}$ are the arcs around rationals a/q with $q\le r$. We will soon discuss how to bound the integral of $\left|S_{\eta_+}(\alpha,x)\right|^2$ over arcs around rationals a/q with $q\le s$, s arbitrary. Here, however, it is best to estimate the integral over $\mathfrak{M}$ using the estimate on $S_{\eta_+}(\alpha,x)$ from (3.3) and (3.7); we obtain a great deal of cancellation, with the effect that, for χ non-trivial, the error term in (3.8) appears only when it gets squared, and thus becomes negligible.

The contribution of the trivial character has an easy approximation, thanks to the fast decay of $\widehat{\eta_\circ}$. We obtain that the major-arc integral (5.1) equals a main term $C_0 C_{\eta_\circ,\eta_*} x^2$, where

$$C_0 = \prod_{p\mid n}\left(1-\frac{1}{(p-1)^2}\right)\cdot \prod_{p\nmid n}\left(1+\frac{1}{(p-1)^3}\right),$$

$$C_{\eta_\circ,\eta_*} = \int_0^\infty\int_0^\infty \eta_\circ(t_1)\eta_\circ(t_2)\eta_*\left(\frac{n}{x}-(t_1+t_2)\right)dt_1dt_2,$$

plus several small error terms. We have already chosen $\eta_\circ$, η_* and x so as to (nearly) maximize $C_{\eta_\circ,\eta_*}$.

It is time to bound the minor-arc integral (5.2). As we said in §5, we must do better than the usual bound (5.3). Since our minor-arc bound (4.16) on $|S_\eta(\alpha,x)|$, $\alpha\sim a/q$, decreases as q increases, it makes sense to use partial summation together with bounds on

$$\int_{\mathfrak{m}_s}|S_{\eta_+}(\alpha,x)|^2 = \int_{\mathfrak{M}_s}|S_{\eta_+}(\alpha,x)|^2 d\alpha - \int_{\mathfrak{M}}|S_{\eta_+}(\alpha,x)|^2 d\alpha,$$

where $\mathfrak{m}_s$ denotes the arcs around a/q, $r<q\le s$, and $\mathfrak{M}_s$ denotes the arcs around all a/q, $q\le s$. We already know how to estimate the integral on $\mathfrak{M}$. How do we bound the integral on $\mathfrak{M}_s$?

In order to do better than the trivial bound $\int_{\mathfrak{M}_s}\le\int_{\mathbb{R}/\mathbb{Z}}$, we will need to use the fact that the series (3.2) defining $S_{\eta_+}(\alpha,x)$ is essentially supported on prime numbers. Bounding the integral on $\mathfrak{M}_s$ is closely related to the problem of bounding

$$\sum_{q\le s}\sum_{\substack{a \bmod q\\(a,q)=1}}\left|\sum_{n\le x} a_n e(a/q)\right|^2 \tag{5.6}$$

efficiently for s considerably smaller than $\sqrt{x}$ and a_n supported on the primes $\sqrt{x}<p\le x$. This is a classical problem in the study of the large sieve. The usual bound on (5.6) (by, for instance, Montgomery's inequality) has a gain of a factor of $2e^\gamma(\log s)/(\log x/s^2)$ relative to the bound of $(x+s^2)\sum_n|a_n|^2$ that one would get from the large sieve without using prime support. Heath-Brown proceeded similarly to bound

$$\int_{\mathfrak{M}_s}|S_{\eta_+}(\alpha,x)|^2 d\alpha \lesssim \frac{2e^\gamma\log s}{\log x/s^2}\int_{\mathbb{R}/\mathbb{Z}}|S_{\eta_+}(\alpha,x)|^2 d\alpha. \tag{5.7}$$

This already gives us the gain of $C(\log s)/\log x$ that we absolutely need, but the constant C is suboptimal; the factor in the right side of (5.7) should really be $(\log s)/\log x$, i.e., C should be 1. We cannot reasonably hope to do better than $2(\log s)/\log x$ in the minor arcs due to what is known as the *parity problem* in sieve theory. As it turns out, Ramaré [52] had given general bounds on the large sieve that were clearly conducive to better bounds on (5.6), though they involved a ratio that was not easy to bound in general.

I used several careful estimations (including [51, Lem. 3.4]) to reduce the problem of bounding this ratio to a finite number of cases, which I then checked by rigorous computation. This approach gave a bound on (5.6) with a factor of size close to $2(\log s)/\log x$. (This solves the large-sieve problem for $s \le x^{0.3}$; it would still be worthwhile to give a computation-free proof for all $s \le x^{1/2-\epsilon}$, $\epsilon > 0$.) It was then easy to give an analogous bound for the integral over $\mathfrak{M}_s$, namely,

$$\int_{\mathfrak{M}_s} |S_{\eta_+}(\alpha, x)|^2 d\alpha \lesssim \frac{2\log s}{\log x} \int_{\mathbb{R}/\mathbb{Z}} |S_{\eta_+}(\alpha, x)|^2 d\alpha,$$

where $\lesssim$ can easily be made precise by replacing $\log s$ by $\log s + 1.36$ and $\log x$ by $\log x + c$, where c is a small constant. Without this improvement, the main theorem would still have been proved, but the required computation time would have been multiplied by a factor of considerably more than $e^{3\gamma} = 5.6499\ldots$.

What remained then was just to compare the estimates on (5.1) and (5.2) and check that (5.2) is smaller for $n \ge 10^{27}$. This final step was just bookkeeping. As we already discussed, a check for $n < 10^{27}$ is easy. Thus ends the proof of the main theorem.

6. Some remarks on computations

There were two main computational tasks: verifying the ternary conjecture for all $n \le C$, and checking the Generalized Riemann Hypothesis for modulus $q \le r$ up to a certain height.

The first task was not very demanding. Platt and I verified in [31] that every odd integer $5 < n \le 8.8 \cdot 10^{30}$ can be written as the sum of three primes. (In the end, only a check for $5 < n \le 10^{27}$ was needed.) We proceeded as follows. Oliveira e Silva, Herzog and Pardi [46]) had already checked that the binary Goldbach conjecture is true up to $4 \cdot 10^{18}$. Given that, all we had to do was to construct a "prime ladder", that is, a list of primes from 3 up to $8.8 \cdot 10^{30}$ such that the difference between any two consecutive primes in the list is at least 4 and at most $4 \cdot 10^{18}$. (This is a known strategy: see [55].) Then, for any odd integer $5 < n \le 8.8 \cdot 10^{30}$, there is a prime p in the list such that $4 \le n - p \le 4 \cdot 10^{18} + 2$. (Choose the largest $p < n$ in the ladder, or, if n minus that prime is 2, choose the prime immediately under that.) By [46] (and the fact that $4 \cdot 10^{18} + 2$ equals $p + q$, where $p = 2000000000000001301$ and $q = 1999999999999998701$ are both prime), we can write $n - p = p_1 + p_2$ for some primes p_1, p_2, and so $n = p + p_1 + p_2$.

Building a prime ladder involves only integer arithmetic, that is, computer manipulation of integers, rather than of real numbers. Integers are something that computers can handle rapidly and reliably. We look for primes for our ladder only among a special set of integers whose primality can be tested deterministically quite quickly (Proth numbers: $k \cdot 2^m + 1$, $k < 2^m$). Thus, we can build a prime ladder by a rigorous, deterministic algorithm that can be (and was) parallelized trivially.

The second computation is more demanding. It consists in verifying that, for every L-function $L(s,\chi)$ with χ of conductor $q \le r = 300000$ (for q even) or $q \le r/2$ (for q odd), all zeroes of $L(s,\chi)$ such that $|\Im(s)| \le H_q = 10^8/q$ (for q odd) and $|\Im(s)| \le H_q = \max(10^8/q, 200 + 7.5 \cdot 10^7/q$ (for q even) lie on the critical line. This was entirely Platt's work; my sole contribution was to request computer time. In fact, he went up to conductor $q \le 200000$ (or twice that for q even); he had already gone up to conductor 100000 in his PhD thesis. The verification took, in total, about 400000 core-hours (i.e., the total number of processor cores used times the number of hours they ran equals 400000; nowadays, a top-of-the-line processor typically has eight cores). In the end, since I used only $q \le 150000$ (or twice that for q even), the number of hours actually needed was closer to 160000; since I could have made do with $q \le 120000$ (at the cost of increasing C to 10^{29} or 10^{30}), it is likely, in retrospect, that only about 80000 core-hours were needed.

Checking zeros of L-functions computationally goes back to Riemann (who did it by hand for the special case of the Riemann zeta function). It is also one of the things that were tried on digital computers in their early days (by Turing [61], for instance; see the exposition in [1]). One of the main issues to be careful about arises whenever one manipulates real numbers via a computer: generally speaking, a computer cannot store an irrational number, and so one cannot say: "computer, give me the sine of that number" and expect a precise result. What one should do is to say: "computer, I am giving you an interval $I = [a/2^k, b/2^k]$; give me an interval $I' = [c/2^\ell, d/2^\ell]$, preferably very short, such that $\sin(I) \subset I'$". This is called interval arithmetic; it is arguably the easiest way to do floating-point computations rigorously.

Processors do not do this natively, and if interval arithmetic is implemented purely on software, computations can be slowed down by a factor of about 100. Fortunately, there are ways of running interval-arithmetic computations partly on hardware, partly on software. Platt has his own library, but there are others online (e.g. PROFIL/BIAS [38]).

Lastly, there were several relatively minor computations embedded in [27–29]. A typical computation was a rigorous version of a "proof by graph" ("the maximum of a function f is clearly less than 4 because I can see it on the screen"). There is a standard way to do this (see, e.g., [60, §5.2]); essentially, the bisection method combines naturally with interval arithmetic. Yet another computation (and not a very small one) was that involved in verifying a large-sieve inequality in an intermediate range (as we discussed in §5).

It may be interesting to note that one of the inequalities used to estimate (4.13) was proven with the help of automatic quantifier elimination [32]. Proving this inequality was a very minor task, both computationally and mathematically; in all likelihood, it is feasible to give a human-generated proof. Still, it is nice to know from first-hand experience that computers can nowadays (pretend to) do something other than just perform numerical computations – and that this is true even in current mathematical practice.

Acknowledgements. Thanks are due to J. Brandes and R. Vaughan for a discussion on a possible ambiguity in the Latin word in [14, p. 298]. Descartes' statement is mentioned (with a translation much like the one given here) in Dickson's *History* [17, Ch. XVIII]. Parts of the present article are based on a previous expository note by the author. The first version of the note appeared online, in English, in an informal venue [30]; later versions were published in Spanish ([25], translated by M. A. Morales and the author, and revised with the help of J. Cilleruelo and M. Helfgott) and French ([26], translated by M. Bilu and revised by the author). Many individuals and organizations should be thanked for their

generous help towards the work summarized here; an attempt at a full list can be found in the acknowledgments sections of [27–29]. Thanks are also due to J. Brandes, K. Gong, R. Heath-Brown, Z. Silagadze, R. Vaughan and T. Wooley, for help with historical questions.

References

[1] A. R. Booker, *Turing and the Riemann hypothesis*, Notices Amer. Math. Soc. **53** (2006), no. 10, 1208–1211.

[2] K. G. Borodzkin, *On the problem of I. M. Vinogradov's constant*, Proc. Third All-Union Math. Conf., vol. 1, Izdat. Akad. Nauk SSSR, Moscow, 1956, p. 3 (Russian).

[3] Y. Buttkewitz, *Exponential sums over primes and the prime twin problem*, Acta Math. Hungar. **131** (2011), no. 1-2, 46–58.

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

[5] ———, *On the estimation of some trigonometrical sums and their application*, Sci. Sinica Ser. A **28** (1985), no. 5, 449–458.

[6] J. R. Chen and T. Z. Wang, *On the Goldbach problem*, Acta Math. Sinica **32** (1989), no. 5, 702–718.

[7] ———, *The Goldbach problem for odd numbers*, Acta Math. Sinica (Chin. Ser.) **39** (1996), no. 2, 169–174.

[8] N. G. Chudakov, *Introduction to the theory of Dirichlet L-functions*, OGIZ, Moscow-Leningrad, 1947 (Russian).

[9] N.G. Chudakov, *On the Goldbach problem*, C. R. (Dokl.) Acad. Sci. URSS, n. Ser. **17** (1937), 335–338 (French).

[10] ———, *On the density of the set of even numbers which are not representable as the sum of two odd primes*, Izv. Akad. Nauk SSSR Ser. Mat. 2 (1938), 25–40.

[11] H. Daboussi, *Effective estimates of exponential sums over primes*, Analytic number theory, Vol. 1 (Allerton Park, IL, 1995), Progr. Math., vol. 138, Birkhäuser Boston, Boston, MA, 1996, pp. 231–244.

[12] H. Daboussi and J. Rivat, *Explicit upper bounds for exponential sums over primes*, Math. Comp. **70** (2001), no. 233, 431–447 (electronic).

[13] H. Davenport, *Multiplicative number theory*, Markham Publishing Co., Chicago, Ill., 1967, Lectures given at the University of Michigan, Winter Term.

[14] R. Descartes, *Œuvres de Descartes publiées par Charles Adam et Paul Tannery sous les auspices du Ministère de l'Instruction publique. Physico-mathematica. Compendium musicae. Regulae ad directionem ingenii. Recherche de la vérité. Supplément à la correspondance. X.*, Paris: Léopold Cerf. IV u. 691 S. 4°, 1908.

[15] J.-M. Deshouillers, *Sur la constante de Šnirel′man*, Séminaire Delange-Pisot-Poitou, 17e année: (1975/76), Théorie des nombres: Fac. 2, Exp. No. G16, Secrétariat Math., Paris, 1977, p. 6.

[16] J.-M. Deshouillers, G. Effinger, H. te Riele, and D. Zinoviev, *A complete Vinogradov 3-primes theorem under the Riemann hypothesis*, Electron. Res. Announc. Amer. Math. Soc. **3** (1997), 99–104.

[17] L. E. Dickson, *History of the theory of numbers. Vol. I: Divisibility and primality.*, Chelsea Publishing Co., New York, 1966.

[18] G. Effinger, *Some numerical implications of the Hardy and Littlewood analysis of the 3-primes problem*, Ramanujan J. **3** (1999), no. 3, 239–280.

[19] T. Estermann, *On Goldbach's Problem: Proof that Almost all Even Positive Integers are Sums of Two Primes*, Proc. London Math. Soc. **S2-44** (1937), no. 4, 307–314.

[20] K. Ford, *Vinogradov's integral and bounds for the Riemann zeta function*, Proc. London Math. Soc. (3) **85** (2002), no. 3, 565–633.

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

[22] A. Granville and O. Ramaré, *Explicit bounds on exponential sums and the scarcity of squarefree binomial coefficients*, Mathematika **43** (1996), no. 1, 73–107.

[23] G. H. Hardy and J. E. Littlewood, *Some problems of 'Partitio numerorum'; III: On the expression of a number as a sum of primes*, Acta Math. **44** (1922), no. 1, 1–70.

[24] D. R. Heath-Brown, *The ternary Goldbach problem*, Rev. Mat. Iberoamericana **1** (1985), no. 1, 45–59.

[25] H. Helfgott, *La conjetura débil de Goldbach*, Gac. R. Soc. Mat. Esp. **16** (2013), no. 4, 709–726.

[26] H. A. Helfgott, *La conjecture de Goldbach ternaire*, Preprint. To appear in Gaz. Math.

[27] ———, *Major arcs for Goldbach's problem*, Preprint. Available at arXiv:1203.5712.

[28] ———, *Minor arcs for Goldbach's problem*, Preprint. Available at arXiv:1205.5252.

[29] ———, *The Ternary Goldbach Conjecture is true*, Preprint.

[30] ———, *The ternary Goldbach conjecture*, 2013, Available at http://valuevar.wordpress.com/2013/07/02/the-ternary-goldbach-conjecture/.

[31] H. A. Helfgott and D. Platt, *Numerical verification of the ternary Goldbach conjecture up to up to* $8.875e30$, To appear in Experiment. Math. Available at arXiv:1305.3062.

[32] H. Hong and Ch. W. Brown, *QEPCAD B – Quantifier elimination by partial cylindrical algebraic decomposition*, May 2011, version 1.62.

[33] M. N. Huxley, *Irregularity in sifted sequences*, J. Number Theory **4** (1972), 437–454.

[34] H. Iwaniec and E. Kowalski, *Analytic number theory*, American Mathematical Society Colloquium Publications, vol. 53, American Mathematical Society, Providence, RI, 2004.

[35] H. Kadiri, *An explicit zero-free region for the Dirichlet L-functions*, Preprint. Available as arXiv:0510570.

[36] ———, *Une région explicite sans zéros pour la fonction ζ de Riemann*, Acta Arith. **117** (2005), no. 4, 303–339.

[37] A. A. Karatsuba, *Basic analytic number theory*, Springer-Verlag, Berlin, 1993, Translated from the second (1983) Russian edition and with a preface by Melvyn B. Nathanson.

[38] O. Knüppel, *PROFIL/BIAS*, February 1999, version 2.

[39] N. M. Korobov, *Estimates of trigonometric sums and their applications*, Uspehi Mat. Nauk **13** (1958), no. 4 (82), 185–192.

[40] M.-Ch. Liu and T. Wang, *On the Vinogradov bound in the three primes Goldbach conjecture*, Acta Arith. **105** (2002), no. 2, 133–175.

[41] K. K. Mardzhanishvili, *On the proof of the Goldbach-Vinogradov theorem (in Russian)*, C. R. (Doklady) Acad. Sci. URSS (N.S.) **30** (1941), no. 8, 681–684.

[42] K. S. McCurley, *Explicit zero-free regions for Dirichlet L-functions*, J. Number Theory **19** (1984), no. 1, 7–32.

[43] H. L. Montgomery, *A note on the large sieve*, J. London Math. Soc. **43** (1968), 93–98.

[44] ———, *Topics in multiplicative number theory*, Lecture Notes in Mathematics, Vol. 227, Springer-Verlag, Berlin, 1971.

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

[46] T. Oliveira e Silva, S. Herzog, and S. Pardi, *Empirical verification of the even Goldbach conjecture, and computation of prime gaps, up to* $4 \cdot 10^{18}$, Accepted for publication in Math. Comp., 2013.

[47] F. W. J. Olver, *Two inequalities for parabolic cylinder functions*, Proc. Cambridge Philos. Soc. **57** (1961), 811–822.

[48] D. Platt, *Numerical computations concerning GRH*, Preprint. Available at arXiv:1305.3087.

[49] O. Ramaré, *Explicit estimates on several summatory functions involving the Moebius function*, Preprint.

[50] ———, *A sharp bilinear form decomposition for primes and Moebius function*, Preprint. To appear in Acta. Math. Sinica.

[51] ———, *On Šnirel′man's constant*, Ann. Scuola Norm. Sup. Pisa Cl. Sci. **22** (1995), no. 4, 645–706.

[52] ———, *Arithmetical aspects of the large sieve inequality*, Harish-Chandra Research Institute Lecture Notes, vol. 1, Hindustan Book Agency, New Delhi, 2009, With the collaboration of D. S. Ramana.

[53] ———, *On Bombieri's asymptotic sieve*, J. Number Theory **130** (2010), no. 5, 1155–1189.

[54] H. Riesel and R. C. Vaughan, *On sums of primes*, Ark. Mat. **21** (1983), no. 1, 46–74.

[55] Y. Saouter, *Checking the odd Goldbach conjecture up to* 10^{20}, Math. Comp. **67** (1998), no. 222, 863–866.

[56] L. Schnirelmann, *Über additive Eigenschaften von Zahlen*, Math. Ann. **107** (1933), no. 1, 649–690.

[57] X. Shao, *A density version of the Vinogradov three primes theorem*, Duke Math. J. **163** (2014), no. 3, 489–512.

[58] Terence Tao, *Every odd number greater than* 1 *is the sum of at most five primes*, Mathematics of Computation (286) **83** (2014), 997–1038.

[59] N. M. Temme and R. Vidunas, *Parabolic cylinder functions: examples of error bounds for asymptotic expansions*, Anal. Appl. (Singap.) **1** (2003), no. 3, 265–288.

[60] W. Tucker, *Validated numerics: A short introduction to rigorous computations*, Princeton University Press, Princeton, NJ, 2011.

[61] A. M. Turing, *Some calculations of the Riemann zeta-function*, Proc. London Math. Soc. (3) **3** (1953), 99–117.

[62] J. G. van der Corput, *Sur l'hypothèse de Goldbach pour presque tous les nombres pairs*, Acta Arith. **2** (1937), 266–290 (French).

[63] R. C. Vaughan, *On the estimation of Schnirelman's constant*, J. Reine Angew. Math. **290** (1977), 93–108.

[64] ———, *Sommes trigonométriques sur les nombres premiers*, C. R. Acad. Sci. Paris Sér. A-B **285** (1977), no. 16, A981–A983.

[65] ———, *Recent work in additive prime number theory*, Proceedings of the International Congress of Mathematicians (Helsinki, 1978), Acad. Sci. Fennica, Helsinki, 1980, pp. 389–394.

[66] ———, *The Hardy-Littlewood method*, second ed., Cambridge Tracts in Mathematics, vol. 125, Cambridge University Press, Cambridge, 1997.

[67] I. M. Vinogradov, *A new method in analytic number theory*, Tr. Mat. Inst. Steklova **10** (1937), 5–122 (Russian).

[68] ———, *The method of trigonometrical sums in the theory of numbers*, Tr. Mat. Inst. Steklova **23** (1947), 3–109 (Russian).

[69] ———, *The method of trigonometrical sums in the theory of numbers*, Interscience Publishers, London and New York, 1954. Translated, revised and annotated by K. F. Roth and Anne Davenport.

[70] ———, *A new estimate of the function* $\zeta(1+it)$, Izv. Akad. Nauk SSSR. Ser. Mat. **22** (1958), 161–164.

[71] A. Weil, *Number theory: An approach through history. From Hammurapi to Legendre*, Birkhäuser Boston, Inc., Boston, MA, 1984.

[72] D. Zinoviev, *On Vinogradov's constant in Goldbach's ternary problem*, J. Number Theory **65** (1997), no. 2, 334–358.

DMA - École Normale Supérieure, 45 rue d'Ulm, F-75230 Paris, France
E-mail: harald.helfgott@ens.fr