THE TERNARY GOLDBACH CONJECTURE

ROBERT J. LEMKE OLIVER AND FRANK THORNE

12. The Ternary Goldbach Conjecture

For an even integer x, write

$$N(x) := \#\{p \leq x \ : n - p \text{ prime}\}.$$

In the previous section[1], we described a heuristic argument that led to the conjecture

$$N(x) \sim \prod_{\ell \nmid x} \left(1 - \frac{2}{\ell}\right) \left(1 - \frac{1}{\ell}\right)^{-2} \prod_{\ell \mid n} \left(1 - \frac{1}{\ell}\right)^{-1} \cdot \frac{x}{(\log x)^2}. \tag{12.1}$$

We also have the

Conjecture 12.1 (Goldbach's conjecture)**.** *We have $\pi_n(x) \geq 1$ for each even $n \geq 4$.*

Although you should think of (12.1) as being a much stronger version of Goldbach's conjecture, you should also note that (12.1) doesn't actually *imply* Goldbach's conjecture. For that, one would need a version of (12.1) for which the error term was completely explicit. For example, suppose hypothetically that someone proved that

$$\left| N(x) - \prod_{\ell \nmid n} \left(1 - \frac{2}{\ell}\right) \left(1 - \frac{1}{\ell}\right)^{-2} \prod_{\ell \mid n} \left(1 - \frac{1}{\ell}\right)^{-1} \int_2^x \frac{1}{(\log t)^2}\, dt \right| \leq \frac{100x}{(\log x)^4} \tag{12.2}$$

for all even $x \geq 4$. Then, Goldbach would be 'morally proved', but one would have to first do the following:

- Prove that the 'main term' on the left side of (12.2) was strictly larger than $\frac{100x}{(\log x)^4}$, provided that $x > M$ for some explicit M.
- Otherwise prove the Goldbach conjecture for all $x \leq M$.

So, for example, if you settled the Goldbach conjecture for all $x > 10^{12}$, then you'd definitely be done: it is an easy matter for a computer to verify Goldbach for all smaller x. And if you settled Goldbach for $x > 10^{20}$, you could expect that a combination of computation, clever shortcuts, and brute force should be enough to carry the day. But what if you settled Goldbach for, say, $x > 10^{10^{34}}$? You'd have to either bring that value of x down *a lot*, or else admire your achievement as it stood.

Goldbach's conjecture remains unsettled, but the following 'ternary' version has been settled:

Conjecture 12.2 (Ternary Goldbach conjecture)**.** *Define*

$$N_3(x) := \#\{p_1, p_2, p_3 \text{ prime} \ \ : \ p_1 + p_2 + p_3 = x\}.$$

Then, we have $N_3(x) \geq 1$ for all odd $x \geq 7$.

Date: December 16, 2019.

[1]to do... something there is funny... choose notation.

As described in the previous section, the ternary Goldbach conjecture has been proved! It was first proved by Hardy and Littlewood for large x, conditionally on GRH; then by Vinogradov, without the GRH assumption; and then (only in 2013!) in full by Helfgott.

In this book we will present a proof of ternary Goldbach for large x, conditionally on GRH. We will borrow heavily from the beautiful treatment by Soundararajan [**?**] in his notes on additive combinatorics.

In fact, we will prove the following:

Theorem 12.3. *As $x \to \infty$ we have*

$$\sum_{n_1+n_2+n_3=x} \Lambda(n_1)\Lambda(n_2)\Lambda(n_3) \sim \frac{x^2}{2}\mathfrak{S}(x), \tag{12.3}$$

where

$$\mathfrak{S}(x) := \prod_{p|x}\left(1 - \frac{1}{(p-1)^2}\right)\prod_{p\nmid x}\left(1 + \frac{1}{(p-1)^3}\right).$$

Note that if $2 \mid x$ then $\mathfrak{S}(x) = 0$, and in this case the right side of (12.5) is to be interpreted as simply $o(x^2)$.

Some preparatory notes, which we leave as exercises. (From an expert's perspective these would all be routine; consider them good practice if you are an aspiring expert!)

- Remember that $\Lambda(n) := \log p$ if p is prime and n is an exact power of p. The contribution of nontrivial prime *powers* to (12.5) is negligible, and (12.5) is equivalent to the statement

$$\sum_{p_1+p_2+p_3=x} (\log p_1)(\log p_2)(\log p_3) \sim \frac{x^2}{2}\mathfrak{S}(x), \tag{12.4}$$

  where the p_i indicate prime numbers.
- By a variant of partial summation, we can further reduce this to

$$\sum_{p_1+p_2+p_3=x} 1 \sim \frac{x^2}{2(\log x)^3}\mathfrak{S}(x), \tag{12.5}$$

  where the p_i indicate prime numbers.
- The singular series $\mathfrak{S}(x)$ is bounded above and below by absolute constants.
- The asymptotic above is *exactly* what you get via a probabilistic argument, assuming the primes are 'random', following the ideas of the previous section.

We now recommend that you set aside this book and spend a good fifteen minutes attempting to prove (12.5). This should prove very enlightening and instructive – as well as utterly futile. Probably you got nowhere, right? *Great.* You are now prepared to appreciate Hardy and Littlewood's genius.

The first step is trivial to prove, but not at all trivial to see.

Theorem 12.4 (Additive Identity = Exponential Sum Integral)**.** *For $\alpha \in \mathbb{R}$, write*

$$e(n\alpha) := e^{2\pi i n\alpha}, \quad f(\alpha) := \sum_{n\le x} \Lambda(n)e(n\alpha).$$

Then, we have

$$\int_0^1 f(\alpha)^3 e(-x\alpha)d\alpha = \sum_{n_1+n_2+n_3=x} \Lambda(n_1)\Lambda(n_2)\Lambda(n_3). \tag{12.6}$$

To prove this, just expand out the left side as

$$\sum_{n_1\le x}\sum_{n_2\le x}\sum_{n_3\le x} \Lambda(n_1)\Lambda(n_2)\Lambda(n_3)\int_0^1 e(n_1\alpha)e(n_2\alpha)e(n_3\alpha)e(-x\alpha)d\alpha,$$

and use the identity that for an integer m we have

$$\int_0^1 e(m\alpha)d\alpha = \begin{cases} 1 & \text{if } m=0,\\ 0 & \text{if } m\neq 0.\end{cases} \tag{12.7}$$

Okay, so what? We are staking the proof on being able to understand $f(\alpha)$. The trivial bound is $|f(\alpha)| < x$, and therefore $\int_0^1 f(\alpha)^3 e(-x\alpha)d\alpha < x^3$, and we are going to have to beat this by a lot.

Example 12.5. Set $\alpha = \frac{1}{4}$. Then

$$f(\alpha) = \sum_{\substack{n\equiv\ 0 \pmod 4\\ n\le x}} \Lambda(n) + i\sum_{\substack{n\equiv 1 \pmod 4\\ n\le x}} \Lambda(n) - \sum_{\substack{n\equiv 2 \pmod 4\\ n\le x}} \Lambda(n) - i\sum_{\substack{n\equiv 3 \pmod 4\\ n\le x}} \Lambda(n).$$

The contribution from the sums with $n \equiv\ 0, 2 \pmod 4$ are negligible, with just the powers of 2 contributing. Their total contribution is just $O(\log x)$. So we can rewrite this as

$$f(\frac{1}{4}) = O(\log x) + i\sum_{\substack{n\equiv 1 \pmod 4\\ n\le x}} \Lambda(n) - i\sum_{\substack{n\equiv 3 \pmod 4\\ n\le x}} \Lambda(n).$$

By the Prime Number Theorem for Arithmetic Progressions, conditional on GRH, we have

$$f(\frac{1}{4}) = O\big(x^{1/2}(\log x)^2\big). \tag{12.8}$$

Example 12.6. Let α and β be arbitrary real numbers with β 'small'. Then,

$$f(\alpha+\beta) - f(\alpha) = \sum_{n\le x}\Lambda(n)\big(e(n(\alpha+\beta)) - e(n\alpha)\big).$$

We have that

$$\big|e(n(\alpha+\beta)) - e(n\alpha)\big| = |e(n\beta)-1| \ll n\beta \le x\beta.$$

So, for example, we can conclude from (12.9) that

$$f(\alpha) = O\big(x^{1/2}(\log x)^2\big)$$

whenever $|\alpha - \frac{1}{4}| < x^{-1/2}$.

Example 12.7. Now set $\alpha = \frac{1}{3}$. Similarly to (12.5) we have

$$f(1/3) = O(\log n) + \omega\sum_{\substack{n\equiv 1 \pmod 3\\ n\le x}} \Lambda(n) + \omega^2\sum_{\substack{n\equiv 2 \pmod 3\\ n\le x}} \Lambda(n),$$

with $\omega = e^{2\pi i/3}$, but now notice an important difference. In (12.5) we had $i + (-i) = 0$, but now we have $\omega + \omega^2 = -1$. By the prime number theorem for arithmetic progressions (again, on GRH), we now have

$$f(\frac{1}{3}) = -\frac{1}{2}x + O\big(x^{1/2}(\log x)^2\big). \tag{12.9}$$

Example 12.8. Suppose $\alpha = \frac{1}{\sqrt{2}}$. Then we get

$$f(\alpha) = O(\sqrt{n}) + \sum_{p \leq x} e^{2\pi i \alpha p} \log p.$$

We don't yet know how to deal with sums like this; clearly we will have to.

We can now explain our basic strategy.

The Circle Method: Basic Strategy.

(1) We start with a problem in 'additive number theory': in how many ways can x be written as a sum of three (five, ten, a hundred, ...) primes (almost-primes, perfect squares, Fibonacci numbers, ...)?

Write the solution as an integral involving an exponential sum similar to (12.6). The integral over [0.1] is really an integral over the circle $\{z \ : |z| = 1\}$, hence the 'circle method'.

(2) Decompose $[0, 1]$ into 'major arcs' – those α which are close to some fraction $\frac{a}{q}$ with small denominator – and the 'minor arcs' (everything else).

(3) Evaluate the major arcs as outlined above. For $f(a/q)$ we will get expressions like (12.9), which will lead to our eventual main term. For $f(\alpha)$ with α very close to a/q, we proceed as in (12.6).

(4) Bound the minor arcs, and prove that they contribute an error term.

This probably looks incredibly daunting – but the reader will be pleasantly surprised.

Our main technical input is the following version of the prime number theorem for arithmetic progressions.

Lemma 12.9. *Let $\chi \pmod q$ be a Dirichlet character, and define*

$$\psi(x, \chi) := \sum_{n \leq x} \Lambda(n)\chi(n).$$

Assume that the Riemann Hypothesis holds for the L-function $L(s, \chi)$. Then, we have

$$\psi(x, \chi) \ll x^{1/2}(\log x)^2$$

for χ nonprincipal (uniformly in χ and q), and

$$\psi(x, \chi) = x + O\big(x^{1/2}(\log(qx))^2\big)$$

for χ principal.

This is where our Generalized Riemann Hypothesis fits in the picture – without GRH, we would not be able to prove nearly such good error terms. *As you read the proof, you should pay attention to where the strength of these error terms gets used!*

Notice also that Lemma 12.9 is presented in more raw form than the usual version of PNTAP. The expression $\psi(x, \chi)$ is what the classical proof directly counts, after which the orthogonality relations and partial summation lead to a count of $\pi(x; q, a)$.

We also will need the following:

Lemma 12.10 (Dirichlet's Approximation Theorem)**.** *Let Q be a positive integer. Then, for any $\alpha \in [0,1]$ we have $|\alpha - a/q| \leq 1/qQ$ for some fraction a/q with $q \leq Q$.*

Proof. The stated inequality is equivalent to $|q\alpha - a| \leq 1/Q$. Look at the numbers $\alpha, 2\alpha, \cdots, Q\alpha$ modulo 1 (more precisely, at their images in $\mathbb{R}/\mathbb{Z}$). Since there are Q such numbers, by the pigeonhole principle some two of them, say $c\alpha$ and $c'\alpha$, must have distance bounded above by $1/Q$. But this implies that $(c-c')\alpha$ is within $1/Q$ of an integer – exactly what we wished to prove.

□

Now we may begin with the proof in earnest. Our first step is an evaluation of $f(\alpha)$ at rational numbers.

Lemma 12.11. *Let a/q be a rational number with $(a,q)=1$. Then, assuming GRH, we have*

$$f(a/q) = \sum_{n \leq x} \Lambda(n) e(na/q) = \frac{\mu(q)}{\phi(q)} x + O(\sqrt{qx}(\log x)^2).$$

Proof. As a first step, we have

$$\sum_{n \leq x} \Lambda(n) e(na/q) = O\big((\log x)^2\big) + \sum_{\substack{n \leq x \\ (n,q)=1}} \Lambda(n) e(na/q).$$

Now, rewrite

$$e(an/q) = \frac{1}{\phi(q)} \sum_{\chi (\operatorname{mod} q)} \overline{\chi(an)} \tau(\chi), \tag{12.10}$$

where $\tau(\chi)$ denotes the Gauss sum

$$\tau(\chi) = \sum_{a (\operatorname{mod} q)} \chi(a) e(a/q), \tag{12.11}$$

with $|\tau(\chi)| \leq \sqrt{q}$ (and with equality when χ is primitive). We therefore obtain

$$\sum_{n \leq x} \Lambda(n) e(na/q) = O\big((\log x)^2\big) + \frac{1}{\phi(q)} \sum_{\chi (\operatorname{mod} q)} \overline{\chi(a)} \tau(\chi) \psi(x, \overline{\chi}). \tag{12.12}$$

By the GRH version of the prime number theorem for arithmetic progressions (Lemma 12.9), we have $|\psi(x,\overline{\chi})| \ll x^{1/2} (\log x)^2$ for each nonprincipal q, and the total contribution of these is $\ll \sqrt{qx}(\log x)^2$. Meanwhile, the contribution of the principal character is

$$\frac{1}{\phi(q)} \tau(\chi_0) \left(x + O(\sqrt{x}(\log x)^2)\right).$$

(Here this involves an evaluation of the Gauss sum (12.11); the details are not difficult.) Putting this all together concludes the proof.

□

Interlude. What does this proof have in common with Greek drama?

The ancient Greeks were the world's first dramatists. One convention which they introduced was *deus ex machina* – the 'god from the machine'. The main characters would foul everything up, landing themselves in an irremediable situation. Following which a character playing a Greek god (the *deus*), would be lowered to the stage using some sort of crane (the *machina*), and then the god would make everything right.

Nowadays, very few audiences would be satisfied with such a conclusion. We are more accustomed to Shakespeare: after the main characters make a mess of everything, no god comes to save them. Rather, the situation degenerates further, and everyone dies. As an audience this satisfies: we want to feel the presence of order and rationality, cause and effect, in the universe.

In the proof above, (12.10) may well look like our *deus ex machina*. A god was lowered onto the stage, it waved its arms about (see (12.12)), and we got something we knew how to handle.

(**to be continued —**)

Lemma 12.12. *Assume GRH, and let $\alpha = a/q + \beta$ with $(a,q) = 1$. Then*

$$f(\alpha) = \frac{\mu(q)}{\phi(q)} \int_0^x e(\beta t)dt + O\left((1 + |\beta| x)\sqrt{qx}(\log x)^2\right).$$

Proof. We have that

$$f(\alpha) = \int_0^X e(t\beta) d\left(\sum_{n \leq t} \Lambda(n) e(an/q)\right) = \int_0^x e(t\beta) d\left(\frac{\mu(q)}{\phi(q)} + E(x, a/q)\right),$$

where the error term $E(x, a/q)$ is the one given in Lemma 12.11. The main term gives the main term of the lemma, and we treat the error term by integration by parts. This error term is

$$E(x, a/q)e(x\beta) - \int_0^x 2\pi i \beta e(t\beta) E(t, a/q) dt,$$

and bounding the integrand by its absolute value immediately yields the lemma. □

Corollary 12.13. *Set $Q = x^{2/3}$, and suppose that $|\alpha - a/q| \leq 1/qQ$ with $(a,q) = 1$, for some $q \leq Q$.*

Then, on GRH, we have

$$f(\alpha) \ll \frac{x}{\phi(q)} + x^{5/6}(\log x)^2.$$

Proof. This is quite immediate from Lemma 12.12. We have

$$f(\alpha) \ll \frac{x}{\phi(q)} + \left(1 + \frac{x}{qQ}\right)\sqrt{qx}(\log x)^2 \ll \frac{x}{\phi(q)} + \left(\sqrt{Qx} + \frac{x^{3/2}}{Q}\right)(\log x)^2.$$

We check that the choice $Q = x^{2/3}$ optimizes the error term (up to the logarithmic factor) and yields the stated bound. □

We now are ready for the heart of the proof.

Definition 12.14. Write $Q = x^{2/3}$ as before. We will say that $\alpha \in [0,1]$ lies on a *major arc* if we have $|\alpha - a/q| \leq 1/qQ$ for some $(a,q) = 1$ and $q \leq (\log x)^{10}$; otherwise, α lies on a *minor arc*.

There is nothing terribly special about the quantity $(\log x)^{10}$, and in other applications the definitions of the major and minor arcs might not be identical.

Lemma 12.15. *If α lies on a minor arc, then we have*[2]

$$f(\alpha) \ll \frac{x}{(\log x)^9}.$$

Proof. We have that $|\alpha - a/q| \leq 1/qQ$ for at least one choice of a and q with $q \leq Q$. By definition of the minor arcs, we have $q > (\log x)^{10}$. Therefore, by Corollary (12.13), the lemma is reduced to showing that $\phi(q) \gg (\log x)^9$.

We'll now cheat a little bit, and claim that it is 'well known' that $\phi(q) \gg q/\log\log q$. (Which it is, to experts anyway.) Given this, if $q > (\log x)^{10}$ we have

$$\phi(q) \gg \frac{(\log x)^{10}}{\log\log\log x} \gg (\log x)^9,$$

as desired. □

Lemma 12.16. *Let $\mathfrak{m}$ denote the set of minor arcs. On GRH, we have*

$$\int_{\mathfrak{m}} |f(\alpha)|^3 d\alpha \ll \frac{x^2}{(\log x)^8}.$$

Note that it does *not* suffice to plug in the bound $|f(\alpha)| \ll \frac{x}{(\log x)^9}$! If you don't see the trick, you could easily go astray.

Proof. Using the previous lemma, we obtain

$$\int_{\mathfrak{m}} |f(\alpha)|^3 d\alpha \ll \frac{x}{(\log x)^9} \int_0^1 |f(\alpha)|^2 d\alpha.$$

Now, opening up the integral we have

$$\begin{aligned}\int_0^1 |f(\alpha)|^2 d\alpha = \int_0^1 f(\alpha)\overline{f(\alpha)} d\alpha &= \int_0^1 \left(\sum_{n\leq x} \Lambda(n) e(n\alpha)\right) \cdot \left(\sum_{m \leq x} \Lambda(m) e(m\alpha)\right) d\alpha \\ &= \sum_{n \leq x} \Lambda(n) \sum_{m\leq x} \Lambda(m) \int_0^1 e(n\alpha)e(-m\alpha) d\alpha \\ &= \sum_{n\leq x} \Lambda(n)^2,\end{aligned}$$

where in the last step we again used the identity (12.7) that got everything started.

We then in turn have

$$\sum_{n\leq x} \Lambda(n)^2 \leq (\log x) \sum_{n \leq x} \Lambda(n) \ll x \log x$$

by the prime number theorem, which completes the proof. □

This is good enough, so we turn attention now to the major arcs. Note that the intervals for different rational numbers are disjoint: more precisely, we can have $|\alpha - a/q| \leq 1/qQ$ for at most one $q \leq (\log x)^{10}$.

[2]The 9 was an 8 in Sound's notes. Double check that I haven't done anything dumb here.

Writing $\mathfrak{M}$ for the set of major arcs, we have

$$\int_{\mathfrak{M}} f(\alpha)^3 e(-x\alpha)d\alpha = \sum_{q\leq(\log x)^{10}} \sum_{\substack{1\leq a\leq q\\(a,q)=1}} \int_{-1/qQ}^{1/qQ} f(a/q+\beta)^3 e\left(-x\left(\frac{a}{q}+\beta\right)\right) d\beta. \tag{12.13}$$

Now, by Lemma 12.12 we have

$$f(a/q+\beta)^3 = \frac{\mu(q)^3}{\phi(q)^3}\left(\int_0^x e(\beta t)dt\right)^3 + O\left(\frac{1}{\phi(q)^2}\left(\int_0^x e(\beta t)dt\right)^2 \cdot (1+|\beta|x)(qx)^{1/2}(\log(qx))^2\right)$$
$$+ O\left((1+|\beta|x)^3(qx)^{3/2}(\log(qx))^6\right).$$

Note that we have

$$\int_0^x e(\beta t)dt \ll \min(x, |\beta|^{-1}).$$

To evaluate the total error contribution to (12.13), we have some cleanup to do, and it is useful to know how to simplify things! Since $q \leq x$, we start by lumping together all the logarithmic terms. As q is small in this case, we can afford to ignore the $\frac{1}{\phi(q)^2}$ factor, replacing it simply by 1. And, we have $q \leq (\log x)^{10}$, which we will use for the positive powers of q appearing above. Finally, note that the sum over a and q is over less than $(\log x)^{20}$ terms.

Therefore, the error in estimating $f(a/q+\beta)^3$ above is bounded above by

$$E(a/q,\beta) \ll \log(x)^{21} \cdot \left(\min(x,|\beta|^{-1}) \cdot (1+|\beta|x)x^{1/2} + (1+|\beta|x)^3 x^{3/2}\right).$$

We integrate over $\beta \in [-1/qQ, 1/qQ]$. We first consider the contribution of those β with $|\beta| \leq 1/x$. For such β, we have

$$E(a/q,\beta) \ll \log(x)^{21}\Big(x \cdot x^{1/2} + x^{3/2}\Big).$$

The set of such β has measure $2/x$, and so (summing over a and q also) the total contribution here is a harmless $x^{1/2}(\log x)^{41}$.

For $\beta > 1/x$, we have

$$\begin{aligned} E(a/q,\beta) &\ll (\log x)^{21} \cdot \left(|\beta|^{-1} \cdot (|\beta|x)x^{1/2} + (|\beta|x)^3 x^{3/2}\right) \\ &= (\log x)^{21}\left(x^{3/2} + |\beta|^3 x^{9/2}\right). \end{aligned}$$

The integral over $\beta \in [-1/qQ, 1/qQ]$, which is contained within $[x^{-2/3}, x^{2/3}]$, is bounded above by

$$\ll (\log x)^{21}\left(x^{3/2} \cdot x^{-2/3} + x^{-8/3} \cdot x^{9/2}\right).$$

That is $O(x^{11/6}(\log x)^{21})$, and summing over a and q we obtain a total contribution $\ll x^{11/6}(\log x)^{41}$.

Therefore, up to an error of $x^{11/6}(\log x)^{41}$, our major arc contribution is

$$\sum_{q\leq(\log x)^{10}} \sum_{\substack{1\leq a\leq q\\(a,q)=1}} \int_{-1/qQ}^{1/qQ} \frac{\mu(q)^3}{\phi(q)^3}\left(\int_0^x e(\beta t)dt\right)^3 e\left(-x\left(\frac{a}{q}+\beta\right)\right) d\beta$$
$$= \sum_{q\leq(\log x)^{10}} \frac{\mu(q)^3}{\phi(q)^3} \sum_{\substack{1\leq a\leq q\\(a,q)=1}} e(-xa/q) \int_{-1/qQ}^{1/qQ} \left(\int_0^x e(\beta t)dt\right)^3 e(-x\beta)\, d\beta.$$

We have

$$\int_{-1/qQ}^{1/qQ} \left(\int_0^x e(\beta t)dt\right)^3 e\left(-x\beta\right) d\beta = \int_{-\infty}^{\infty} \left(\int_0^x e(\beta t)dt\right)^3 e\left(-x\beta\right) d\beta \ + O(q^2Q^2),$$

because we have $|\int_0^x e(\beta t)dt| < 2|\beta|^{-1}$. Summing up to $q = (\log x)^{10}$ we again introduce a harmless error term, so that the contribution of the major arcs is reduced to

$$\sum_{q \le (\log x)^{10}} \frac{\mu(q)^3}{\phi(q)^3} \sum_{\substack{1 \le a \le q \\ (a,q)=1}} e(-xa/q) \times \int_{-\infty}^{\infty} \left(\int_0^x e(\beta t)dt\right)^3 e\left(-x\beta\right) d\beta.$$

Notice that the sum and the integral are completely separate!

We have the following:

Proposition 12.17. *We have*

$$\int_{-\infty}^{\infty} \left(\int_0^x e(\beta t)dt\right)^3 e\left(-x\beta\right) d\beta = \frac{x^2}{2}. \tag{12.14}$$

Proof. Although this can be evaluated directly, a change of variables nicely illustrates the structure here. Set $u = tx$, to see that our integral equals

$$\int_{-\infty}^{\infty} \left(x \int_0^1 e(\beta xu)du\right)^3 e(-x\beta)d\beta,$$

and then $v = \beta x$, so that we are evaluating

$$x^2 \int_{-\infty}^{\infty} \left(\int_0^1 e(vu)du\right)^3 e(-v)dv.$$

We just need to show that integral equals $\frac{1}{2}$. Giving a *motivated* proof of this fact would involve a somewhat lengthy (but interesting!) digression, so we invite the reader to gut out the details herself (or, better yet, to study a lot of Fourier analysis!)

□

The sum over q we 'extend to infinity' in the following sense. We need a bound for

$$\sum_{q > (\log x)^{10}} \frac{\mu(q)^3}{\phi(q)^3} \sum_{\substack{1 \le a \le q \\ (a,q)=1}} e(-xa/q).$$

Since there are $\phi(q)$ summands a, this is bounded above in absolute value by

$$\sum_{q > (\log x)^{10}} \frac{\mu(q)^2}{\phi(q)^2} \ll \sum_{q > (\log x)^{10}} \frac{\mu(q)^2}{q^2} \cdot (\log\log q)^2 \ll (\log x)^{-9}.$$

So, up to this error term, we may replace our sum by

$$\sum_{q=1}^{\infty} \frac{\mu(q)^3}{\phi(q)^3} \sum_{\substack{1 \le a \le q \\ (a,q)=1}} e(-xa/q). \tag{12.15}$$

The key thing to notice here is that the summand is *multiplicative in q.*

Proposition 12.18. *The 'Ramanujan sum'*

$$S(x,q) := \sum_{\substack{1\leq a\leq q\\(a,q)=1}} e(-xa/q)$$

is multiplicative in q, and for prime p we have

$$S(x,p) = \begin{cases} p-1 & \text{if } p \mid x,\\ -1 & \text{if } p \nmid x.\end{cases}$$

Proof. The evaluation of $S(x,p)$ is essentially immediate. To see multiplicativity, we use the Chinese remainder theorem. If q and q' are coprime, then there is a ring isomorphism

$$\begin{aligned}(\mathbb{Z}/q\mathbb{Z}) \times (\mathbb{Z}/q'\mathbb{Z}) &\to \mathbb{Z}/qq'\mathbb{Z}\\ (a,a') &\to aq' + a'q.\end{aligned}$$

This is not difficult to prove from scratch; this map inverts the map

$$a \pmod{qq'} \mapsto \big(a \pmod{q}, a \pmod{q'}\big)$$

which is a ring homomorphism by construction, which is injective because q and q' are coprime, and which is therefore surjective because both sides have the same size.

We therefore have that

$$\begin{aligned}S(x,qq') = \sum_{\substack{1\leq b\leq qq'\\(b,qq')=1}} e(-xb/qq') &= \sum_{\substack{1\leq a\leq q\\(a,q)=1}} \sum_{\substack{1\leq a'\leq q'\\(a,q')=1}} e\left(-x\frac{aq'+a'q}{qq'}\right)\\ &= \sum_{\substack{1\leq a\leq q\\(a,q)=1}} \sum_{\substack{1\leq a'\leq q'\\(a,q')=1}} e(-xa/q)e(-xa'/q'),\end{aligned}$$

as desired. ∎

Therefore, we may write the sum (12.15) in the form

$$\begin{aligned}&\prod_{p\mid x}\left(1+\frac{-1}{(p-1)^3}\cdot(p-1)\right) \times \prod_{p\nmid x}\left(1+\frac{-1}{(p-1)^3}\cdot(-1)\right)\\ =&\prod_{p\mid x}\left(1+\frac{-1}{(p-1)^2}\right) \times \prod_{p\nmid x}\left(1+\frac{1}{(p-1)^3}\right),\end{aligned}$$

which is *exactly* our singular series $\mathfrak{S}(x)$.

Putting all of this together, conditionally on GRH, we obtain that

$$\sum_{n_1+n_2+n_3=x} \Lambda(n_1)\Lambda(n_2)\Lambda(n_3) \sim \frac{x^2}{2}\mathfrak{S}(x) + O\big(x^2(\log x)^{-9}\big), \tag{12.16}$$

as desired.

12.1. **What is the circle method good for?** As you may guess, the circle method is quite flexible and adaptable, and can be used to solve problems of the following nature.

Problem. For each large n, in how many ways can we write n as the sum

$$n = n_1 + n_2 + \cdots + n_k,$$

where each n_i belongs to some 'special' set $\mathcal{S}_i$?

It is required that we be able to estimate the distribution of $\mathcal{S}_i$ in arithmetic progressions. If we can do that, then the method works *in principle*, and the devil is in the details. For example, you might try to prove that every large integer n can be represented as a sum of *four* primes[3], or of ten integer squares. Here are two other examples of problems where the circle method has succeeded.

Theorem 12.19 (Waring's problem)**.** *For each integer $k \geq 1$, there exists an integer $N = N(k)$ such that the following is true:*

Every positive integer n can be written as the sum of N nonnegative kth powers.

A favorite example, obtained by Hardy and Littlewood, concerns the *partition function.* For a positive integer n, a *partition* of n is any multiset of positive integers which sum to n, and $p(n)$ denotes the number of partitions of n. For example, $p(4) = 5$ because

$$4 = 3 + 1 = 2 + 2 = 2 + 1 = 1 + 1 + 1 + 1.$$

There are a huge number of theorems and conjectures concerning the partition function, as well as fascinating connections to the theory of *modular forms.* For example it is known that if $n \equiv 4 \pmod 5$, then $p(n)$ must be divisible by 5.

Perhaps the most natural question is to estimate $p(n)$, and this was done by Hardy and Ramanujan.

Theorem 12.20 (Hardy-Ramanujan)**.** *We have*

$$p(n) \sim \frac{1}{4n\sqrt{3}} \exp\left(\pi\sqrt{\frac{2n}{3}}\right).$$

[3]You can run all the machinery again; alternatively, do you see a way to cheat?

Exercises.

1. (a) Describe a heuristic argument for Theorem 12.3, based on the ideas behind the Hardy-Littlewood prime tuple conjecture.

(b) Using your heuristic argument, conjecture an asymptotic formula for

$$\sum_{n_1+n_2+n_3+n_4=x} \Lambda(n_1)\Lambda(n_2)\Lambda(n_3)\Lambda(n_4).$$

(c) Assuming GRH, prove your conjecture.

2. In Definition 12.14 we used the inequality $q \leq (\log x)^{10}$ as the cutoff for the definition of the major arcs.

(a) Suppose we used $q \leq (\log x)^m$ instead; show that we would have obtained an error term of $O\big(x^2(\log x)^{-m+1}\big)$ in (12.16) instead.

(b) By choosing $q = x^c$ for some $c > 0$, is it possible to obtain a power saving error term in (12.16)? If so, then how strong of an error term can one obtain?

3. Attempt to use this machinery to prove the binary Goldbach conjecture, conditionally on GRH. Fail. Describe explicitly what step(s) go wrong.