Math 571 Chapter 7 The Ternary Goldbach Problem

Robert C. Vaughan

January 13, 2025

- Christian Goldbach was a German mathematician who was a professor of mathematics and history in St Petersburg.

- Christian Goldbach was a German mathematician who was a professor of mathematics and history in St Petersburg.
- On 7 June 1742, from Moscow, he wrote a letter to Euler (letter XLIII) (a copy of which I will put on the next page) in which he stated the following conjecture.

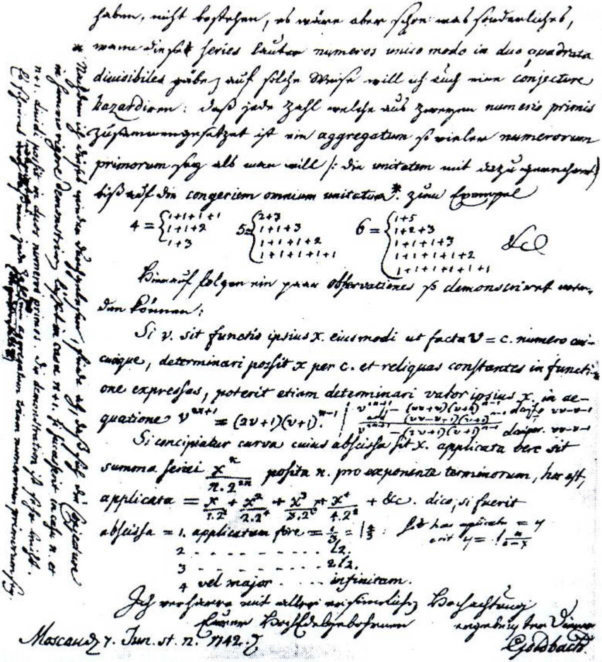
- Christian Goldbach was a German mathematician who was a professor of mathematics and history in St Petersburg.
- On 7 June 1742, from Moscow, he wrote a letter to Euler (letter XLIII) (a copy of which I will put on the next page) in which he stated the following conjecture.
- *Every integer which can be written as the sum of two primes, can also be written as the sum of as many primes as one wishes, until all terms are units.*

- Christian Goldbach was a German mathematician who was a professor of mathematics and history in St Petersburg.
- On 7 June 1742, from Moscow, he wrote a letter to Euler (letter XLIII) (a copy of which I will put on the next page) in which he stated the following conjecture.
- *Every integer which can be written as the sum of two primes, can also be written as the sum of as many primes as one wishes, until all terms are units.*
- In the margin he than added a second conjecture.

- Christian Goldbach was a German mathematician who was a professor of mathematics and history in St Petersburg.
- On 7 June 1742, from Moscow, he wrote a letter to Euler (letter XLIII) (a copy of which I will put on the next page) in which he stated the following conjecture.
- *Every integer which can be written as the sum of two primes, can also be written as the sum of as many primes as one wishes, until all terms are units.*
- In the margin he than added a second conjecture.
- *Every integer greater than 2 can be written as the sum of three primes.*

- Christian Goldbach was a German mathematician who was a professor of mathematics and history in St Petersburg.
- On 7 June 1742, from Moscow, he wrote a letter to Euler (letter XLIII) (a copy of which I will put on the next page) in which he stated the following conjecture.
- *Every integer which can be written as the sum of two primes, can also be written as the sum of as many primes as one wishes, until all terms are units.*
- In the margin he than added a second conjecture.
- *Every integer greater than 2 can be written as the sum of three primes.*
- Of course he took 1 to be prime. In a letter dated 30 June 1742 Euler reminded Goldbach of an earlier conversation they had in which Goldbach had stated a third conjecture that

- Christian Goldbach was a German mathematician who was a professor of mathematics and history in St Petersburg.
- On 7 June 1742, from Moscow, he wrote a letter to Euler (letter XLIII) (a copy of which I will put on the next page) in which he stated the following conjecture.
- *Every integer which can be written as the sum of two primes, can also be written as the sum of as many primes as one wishes, until all terms are units.*
- In the margin he than added a second conjecture.
- *Every integer greater than 2 can be written as the sum of three primes.*
- Of course he took 1 to be prime. In a letter dated 30 June 1742 Euler reminded Goldbach of an earlier conversation they had in which Goldbach had stated a third conjecture that
- *Every even number is the sum of two primes* and Euler pointed out that this would follow from the second conjecture since to represent an even number one of the three primes has to be 2.


haben, nicht bestehen, es wäre aber schon mal sonderlich, wenn dieselbe series lauter numeros unico modo in duo quadrata divisibiles geben würde. Auf solche Weise will ich auch eine conjecture hazardiren: daß jede Zahl welche aus zweyen numeris primis zusammengesetzt ist ein aggregatum so vieler numerorum primorum sey als man will (die unitatem mit dazu gerechnet) bis auf die congeriem omnium unitatum.* zum Exempel

$$4=\begin{cases}1+1+1+1\\1+1+2\\1+3\end{cases}\quad 5=\begin{cases}2+3\\1+1+3\\1+1+1+2\\1+1+1+1+1\end{cases}\quad 6=\begin{cases}1+5\\1+2+3\\1+1+1+3\\1+1+1+1+2\\1+1+1+1+1+1\end{cases}\quad \&c$$

Hierauf folgen ein paar observationes so demonstrirt werden können:

Si v. sit functio ipsius x. eiusmodi ut facta v = c. numero cuicunque, determinari possit x per c. et reliquas constantes in functione expressas, poterit etiam determinari valor ipsius x. in aequatione $v^{2x+1}=(2v+1)(v+1)^{x-1}$ ...

Si concipiatur curva cuius abscissa sit x. applicata vero sit summa seriei $\frac{x^n}{n.2^n}$ posita n. pro exponente terminorum, hoc est, applicata $=\frac{x}{1.2}+\frac{x^2}{2.2^2}+\frac{x^3}{3.2^3}+\frac{x^4}{4.2^4}+$ &c. dico, si fuerit abscissa = 1. applicatam fore $=\frac{1}{2}=l\frac{2}{1}$ ...

2 . . . . $l2$.

3 . . . . $2l2$.

4 vel major . . . infinitam.

Ich verharre mit aller ersinnlichen Hochachtung
Euer Hochedelgebohren
ergebenster Diener
Goldbach

Moscau d. 7. Jun. st. n. 1742.

*Nachdem ich dieses wieder durchgelesen, finde ich, daß sich die conjecture in summo rigore demonstriren lässet in casu n+1, si successerit in casu n et n+1 dividi possit in duos numeros primos. Die demonstration ist sehr leicht. Es scheinet wenigstens, daß eine jede Zahl, die grösser ist als 2, ein aggregatum trium numerorum primorum sey.

- The first assertion that if a number n could be written as a sum of two primes, then it could also be written as the sum of k primes for any k with $2 \le k \le n$ is curious, and as far as I am aware, has never been addressed. Of course for this it is essential to include 1. Without 1 one needs $k \le n/2$. I suspect that either way it is likely to be amenable to modern methods, at least if one starts with three or four primes rather than two.

- The first assertion that if a number n could be written as a sum of two primes, then it could also be written as the sum of k primes for any k with $2 \le k \le n$ is curious, and as far as I am aware, has never been addressed. Of course for this it is essential to include 1. Without 1 one needs $k \le n/2$. I suspect that either way it is likely to be amenable to modern methods, at least if one starts with three or four primes rather than two.
- Today we would state these conjectures as follows. *Every even integer greater than* 2 *can be written as the sum of two primes.*
  Every odd integer greater than 5 *can be written as the sum of three primes.*

- The first assertion that if a number n could be written as a sum of two primes, then it could also be written as the sum of k primes for any k with $2 \le k \le n$ is curious, and as far as I am aware, has never been addressed. Of course for this it is essential to include 1. Without 1 one needs $k \le n/2$. I suspect that either way it is likely to be amenable to modern methods, at least if one starts with three or four primes rather than two.
- Today we would state these conjectures as follows. *Every even integer greater than* 2 *can be written as the sum of two primes.*
  Every odd integer greater than 5 *can be written as the sum of three primes.*
- These have become known as the Goldbach binary and ternary problems.

- There is nothing of consequence in the literature until 1871.

- There is nothing of consequence in the literature until 1871.
- Spottiswoode, then President of the London Mathematical Society, in his account of communications received during the meeting of 9th November 1871 describes at some length researches that Sylvester had been undertaking on the behaviour of

$$R(n) = \mathrm{card}\{p_1, p_2 : p_1 + p_2 = n\} \tag{1}$$

when n is even.

- In modern notation Sylvester asserts that probabilistic arguments suggest that

$$S(n) = \pi(n) \prod_{\substack{p \le \sqrt{n} \\ p \nmid n}} \frac{p-2}{p-1} \tag{2}$$

should be a good approximation to $R(n)$, and further asserts that this is confirmed by the known calculations.

- In modern notation Sylvester asserts that probabilistic arguments suggest that

$$S(n) = \pi(n) \prod_{\substack{p \le \sqrt{n} \\ p \nmid n}} \frac{p-2}{p-1} \tag{2}$$

should be a good approximation to $R(n)$, and further asserts that this is confirmed by the known calculations.

- The product here is quite interesting. A simple argument based on the observation that a number x is divisible by p with probability $\frac{1}{p}$ leads instead to the expression

$$n \left(\prod_{\substack{p \le \sqrt{n} \\ p \nmid n}} \frac{p-2}{p} \right) \prod_{p \mid n} \frac{p-1}{p}. \tag{3}$$

- It turns out that (2) is bad and (3) is worse. However it is interesting and curious that Sylvester should find the product

$$\prod_{\substack{p\le\sqrt{n}\\ p\nmid n}}\frac{p-2}{p-1}.$$

- It turns out that (2) is bad and (3) is worse. However it is interesting and curious that Sylvester should find the product

$$\prod_{\substack{p\le\sqrt{n}\\ p\nmid n}}\frac{p-2}{p-1}.$$

- Of course, the prime number theorem was twenty odd years in the future, and it would be another three years before Mertens theorems

- It turns out that (2) is bad and (3) is worse. However it is interesting and curious that Sylvester should find the product

$$\prod_{\substack{p\le\sqrt{n}\\ p\nmid n}}\frac{p-2}{p-1}.$$

- Of course, the prime number theorem was twenty odd years in the future, and it would be another three years before Mertens theorems
- The underlying difficulty with probabilistic methods is that the series

$$\sum_p\frac{1}{p}$$

diverges.

- Armed with the prime number theorem it is not hard to show that for even n

$$S(n) \sim 2e^{-\gamma} C \frac{\pi(n)}{\log n} \prod_{\substack{p|n \\ p>2}} \frac{p-1}{p-2}$$

where C is the, so called, *twin prime constant*

$$C = 2 \prod_{p>2} \left(1 - \frac{1}{(p-1)^2}\right)$$

- Armed with the prime number theorem it is not hard to show that for even n

$$S(n) \sim 2e^{-\gamma} C \frac{\pi(n)}{\log n} \prod_{\substack{p|n \\ p>2}} \frac{p-1}{p-2}$$

where C is the, so called, *twin prime constant*

$$C = 2 \prod_{p>2} \left(1 - \frac{1}{(p-1)^2}\right)$$

- and to deduce as Landau [1900] did in reference to similar work of Stäckel [1896] that

$$\sum_{n \le x} R(n) \sim \frac{x^2}{2(\log x)^2}$$

whereas

$$\sum_{n \le x} S(n) \sim 2e^{-\gamma} \frac{x^2}{2(\log x)^2}, \quad 2e^{-\gamma} = 1.1229....$$

Hardy and Ramanujan

- Two substantial lines of attack arose almost simultaneously. Sieve methods we have already seen. The other, the seminal paper of Hardy and Ramanujan (1916) on partitions, does not mention Goldbach.

Hardy and Ramanujan

- Two substantial lines of attack arose almost simultaneously. Sieve methods we have already seen. The other, the seminal paper of Hardy and Ramanujan (1916) on partitions, does not mention Goldbach.
- The idea is that for functions $R(n)$ of interest

$$f(z) = \sum_{n=0}^{\infty} R(n) z^n$$

converges for $|z| < 1$ but has singularities on $|z| = 1$. By the Cauchy integral formula

$$R(n) = \frac{1}{2\pi i} \int_{\mathcal{C}} f(z) z^{-n-1} dz$$

where $\mathcal{C} = \{\rho e^{2\pi i\theta} : 0 \le \theta \le 1\}$ and $0 < \rho < 1$, which can be approximated near singularities.

Hardy and Ramanujan

- Typically for functions of arithmetical interest the behaviour of $f(z)$ can be ascertained quite precisely if

$$z = re(a/q + \beta) \quad e(\alpha) = e^{2\pi i\alpha}$$

with r "close" to 1 but β "small" and q "not too large".

Hardy and Ramanujan

- Typically for functions of arithmetical interest the behaviour of $f(z)$ can be ascertained quite precisely if

$$z = re(a/q + \beta) \quad e(\alpha) = e^{2\pi i\alpha}$$

with r "close" to 1 but β "small" and q "not too large".

- Suppose that $R(n)$ is the number of solutions of $x_1^2 + \cdots x_s^2 = n$ with $x_j \geq 0$. Then

$$f(z) = \sum_{n=0}^{\infty} R(n)z^n = g(z)^s \text{ where } g(z) = \sum_{n=0}^{\infty} z^{n^2}.$$

Hardy and Ramanujan

- Typically for functions of arithmetical interest the behaviour of $f(z)$ can be ascertained quite precisely if

$$z = re(a/q + \beta) \quad e(\alpha) = e^{2\pi i\alpha}$$

with r "close" to 1 but β "small" and q "not too large".

- Suppose that $R(n)$ is the number of solutions of $x_1^2 + \cdots x_s^2 = n$ with $x_j \geq 0$. Then

$$f(z) = \sum_{n=0}^{\infty} R(n) z^n = g(z)^s \text{ where } g(z) = \sum_{n=0}^{\infty} z^{n^2}.$$

- Let z be as above and let us sort the terms according to their residue class modulo q. Then

$$g(z) = \sum_{n=0}^{\infty} z^{n^2} = \sum_{m=1}^{q} e(am^2/q) \sum_{n \equiv m \bmod q} r^{n^2} e(\beta n^2).$$

Hardy and Ramanujan

- $$g(z) = \sum_{n=0}^{\infty} z^{n^2} = \sum_{m=1}^{q} e(am^2/q) \sum_{n \equiv m \bmod q} r^{n^2} e(\beta n^2).$$

Hardy and Ramanujan

- $g(z) = \sum_{n=0}^{\infty} z^{n^2} = \sum_{m=1}^{q} e(am^2/q) \sum_{n \equiv m \bmod q} r^{n^2} e(\beta n^2).$
- When r is close to 1 and β is small we can approximate the sum over n by an integral and obtain

$$g(z) \sim q^{-1} S(q, a) \Gamma(3/2)(1 - re(\beta))^{-1/2}.$$

Hardy and Ramanujan

- $g(z) = \sum_{n=0}^{\infty} z^{n^2} = \sum_{m=1}^{q} e(am^2/q) \sum_{n \equiv m \bmod q} r^{n^2} e(\beta n^2).$
- When r is close to 1 and β is small we can approximate the sum over n by an integral and obtain

$$g(z) \sim q^{-1} S(q,a) \Gamma(3/2)(1 - re(\beta))^{-1/2}.$$

- Here $S(q,a)$ is the Gauss sum $S(q,a) = \sum_{m=1}^{q} e(am^2/q)$.

Hardy and Ramanujan

- $g(z) = \sum_{n=0}^{\infty} z^{n^2} = \sum_{m=1}^{q} e(am^2/q) \sum_{n \equiv m \bmod q} r^{n^2} e(\beta n^2).$
- When r is close to 1 and β is small we can approximate the sum over n by an integral and obtain

$$g(z) \sim q^{-1} S(q,a) \Gamma(3/2)(1 - re(\beta))^{-1/2}.$$

- Here $S(q,a)$ is the Gauss sum $S(q,a) = \sum_{m=1}^{q} e(am^2/q)$.
- This estimate can be made sufficiently precise that it is of utility on the whole of $\mathcal{C}$.

Hardy and Ramanujan

- $g(z) = \sum_{n=0}^{\infty} z^{n^2} = \sum_{m=1}^{q} e(am^2/q) \sum_{n \equiv m \bmod q} r^{n^2} e(\beta n^2).$
- When r is close to 1 and β is small we can approximate the sum over n by an integral and obtain

$$g(z) \sim q^{-1} S(q,a) \Gamma(3/2)(1 - re(\beta))^{-1/2}.$$

- Here $S(q,a)$ is the Gauss sum $S(q,a) = \sum_{m=1}^{q} e(am^2/q)$.
- This estimate can be made sufficiently precise that it is of utility on the whole of $\mathcal{C}$.
- In other problems, such as Goldbach or Waring the approximation for $g(z)$ was only good for a small subset of $\mathcal{C}$ and a new idea was required.

Hardy and Ramanujan

- $g(z) = \sum_{n=0}^{\infty} z^{n^2} = \sum_{m=1}^{q} e(am^2/q) \sum_{n \equiv m \bmod q} r^{n^2} e(\beta n^2).$
- When r is close to 1 and β is small we can approximate the sum over n by an integral and obtain

$$g(z) \sim q^{-1} S(q,a) \Gamma(3/2)(1 - re(\beta))^{-1/2}.$$

- Here $S(q,a)$ is the Gauss sum $S(q,a) = \sum_{m=1}^{q} e(am^2/q)$.
- This estimate can be made sufficiently precise that it is of utility on the whole of $\mathcal{C}$.
- In other problems, such as Goldbach or Waring the approximation for $g(z)$ was only good for a small subset of $\mathcal{C}$ and a new idea was required.
- The division of $\mathcal{C}$ into good and bad arcs lead to the terms "major arcs" and "minor arcs".

Hardy and Litlewood

- In 1919 Hardy and Littlewood set themselves the task of developing the fundamental ideas of the Hardy and Ramanujan paper. This eventually saw the light of day as the series of eight papers with the generic title "On some problems of partitio numerorum", the first two of which are on Waring's problem, and the seventh of which never appeared in print.

Hardy and Litlewood

- In 1919 Hardy and Littlewood set themselves the task of developing the fundamental ideas of the Hardy and Ramanujan paper. This eventually saw the light of day as the series of eight papers with the generic title "On some problems of partitio numerorum", the first two of which are on Waring's problem, and the seventh of which never appeared in print.
- The first questions they examined were the Goldbach conjectures. Eventually they realised that they could only make progress by assuming the generalised Riemann hypothesis and they deferred this work until their method had established its provenance with unconditional theorems.

Hardy and Litlewood

- In 1919 Hardy and Littlewood set themselves the task of developing the fundamental ideas of the Hardy and Ramanujan paper. This eventually saw the light of day as the series of eight papers with the generic title "On some problems of partitio numerorum", the first two of which are on Waring's problem, and the seventh of which never appeared in print.
- The first questions they examined were the Goldbach conjectures. Eventually they realised that they could only make progress by assuming the generalised Riemann hypothesis and they deferred this work until their method had established its provenance with unconditional theorems.
- However papers III (1922) and V (1924) are concerned with the Goldbach conjectures.

Hardy and Litlewood

- Hardy and Littlewood used the generating function

$$f(z) = g(z)^s, \quad g(z) = \sum_p (\log p) z^p.$$

Hardy and Litlewood

- Hardy and Littlewood used the generating function

$$f(z) = g(z)^s, \quad g(z) = \sum_p (\log p) z^p.$$

- To describe these results I am going to make an innovation that only came later, due to Vinogradov. Let

$$S(\alpha) = \sum_{p \le n} (\log p) e(\alpha p)$$

Then

$$r_s(n) = \sum_{\substack{p_1,\dots,p_s \\ p_1+\dots+p_s=n}} \log p_1 \dots \log p_s = \int_0^1 S(\alpha)^s e(-\alpha n) d\alpha.$$

Hardy and Littlewood

- If we sort the primes counted by F according to their residue classes modulo q, and we apply results that follow from the generalised Riemann hypothesis, when $(q, a) = 1$,

$$S(a/q + \beta) = \frac{\mu(q)}{\phi(q)} \sum_{m=2}^{n} e(\beta m) + O\left((q + qn|\beta|)^{\frac{1}{2}} n^{\frac{1}{2}+\varepsilon}\right).$$

Hardy and Littlewood

- If we sort the primes counted by F according to their residue classes modulo q, and we apply results that follow from the generalised Riemann hypothesis, when $(q,a)=1$,

$$S(a/q+\beta)=\frac{\mu(q)}{\phi(q)}\sum_{m=2}^{n}e(\beta m)+O\left((q+qn|\beta|)^{\frac12}n^{\frac12+\varepsilon}\right).$$

- Dirichlet's theorem on diophantine approximation says that, given $Q\ge1$ and $\alpha\in\mathbb{R}$, there are $q\le Q$ and a with $(q,a)=1$ so that $|\alpha-a/q|\le q^{-1}Q^{-1}$. Let $\beta=\alpha-a/q$. Then the error term above is

$$O\left((Q+n/Q)^{\frac12}n^{\frac12+\varepsilon}\right)$$

and the optimal choice $Q=n^{\frac12}$ gives $O\big(n^{\frac34+\varepsilon}\big)$.

Hardy and Littlewood

- Thus Hardy and Littlewood were able to treat $r_s(n)$ whenever $s \geq 3$ and they established, on the generalised Riemann hypothesis, that, when $n \equiv s \pmod 2$,

$$r_s(n) \sim \frac{n^{s-1}}{(s-1)!}\mathfrak{S}_s(n)$$

where

$$\mathfrak{S}_s(n) = \left(\prod_{p\nmid n}\left(1+\frac{(-1)^{s+1}}{(p-1)^s}\right)\right)\prod_{p\mid n}\left(1+\frac{(-1)^s}{(p-1)^{s-1}}\right).$$

Hardy and Littlewood

- When $s = 2$ they were unable to prove anything quite as precise but they could establish the following

$$\sum_{\substack{m=1 \\ 2|m}}^{n} \left(r_2(m) - m\mathfrak{S}_2(m)\right)^2 = O\left(n^{\frac{5}{2}+\varepsilon}\right)$$

where

$$\mathfrak{S}_2(n) = C \prod_{\substack{p|n \\ p>2}} \left(\frac{p-1}{p-2}\right).$$

Hardy and Littlewood

- When $s = 2$ they were unable to prove anything quite as precise but they could establish the following

$$\sum_{\substack{m=1 \\ 2|m}}^{n} \left(r_2(m) - m\mathfrak{S}_2(m)\right)^2 = O\left(n^{\frac{5}{2}+\varepsilon}\right)$$

where

$$\mathfrak{S}_2(n) = C \prod_{\substack{p|n \\ p>2}} \left(\frac{p-1}{p-2}\right).$$

- This is, perhaps, the strongest evidence we have that for even n,

$$r_2(n) \sim n\mathfrak{S}_2(n).$$

Hardy and Littlewood

- Of course, why stop there. How good an error term should one expect? Well, one could speculate that

$$r_2(n) = n\mathfrak{S}_2(n) + O\big(n^{\frac{1}{2}+\varepsilon}\big)$$

and if true, then this would be essentially best possible.

Hardy and Littlewood

- Of course, why stop there. How good an error term should one expect? Well, one could speculate that

$$r_2(n) = n\mathfrak{S}_2(n) + O\big(n^{\frac{1}{2}+\varepsilon}\big)$$

  and if true, then this would be essentially best possible.
- Montgomery and Vaughan [1973] have proved unconditionally that

$$\sum_{\substack{m=1\\2|m}}^{n} \big(r_2(m) - m\mathfrak{S}_2(m)\big)^2 = \Omega\left(n^2(\log n)^2\right).$$

Hardy and Littlewood

- Returning to

$$\sum_{\substack{m=1\\2|m}}^{n} \left(r_2(m) - m\mathfrak{S}_2(m)\right)^2 = O\left(n^{\frac{5}{2}+\varepsilon}\right).$$

it follows quite easily that the exceptional set

$$E(x) = \operatorname{card}\{m : 2|m, m \le x, r_2(m) \ne 0\}$$

satisfies

$$E(x) \ll x^{\frac{1}{2}+\varepsilon}.$$

Hardy and Littlewood

- Returning to

$$\sum_{\substack{m=1\\2|m}}^{n} \left(r_2(m) - m\mathfrak{S}_2(m)\right)^2 = O\left(n^{\frac{5}{2}+\varepsilon}\right).$$

it follows quite easily that the exceptional set

$$E(x) = \operatorname{card}\{m : 2|m, m \le x, r_2(m) \ne 0\}$$

satisfies

$$E(x) \ll x^{\frac{1}{2}+\varepsilon}.$$

- Of course, this assumes the generalised Riemann hypothesis.

Vinogradov

- In 1937 Vinogradov proved the following.

Theorem 1 (Vinogradov 1937)

Let

$$S(\alpha) = \sum_{p \le n} e(\alpha p).$$

Suppose that $q \in \mathbb{N}$, $a \in \mathbb{Z}$, $(q, a) = 1$ *and* $|\alpha - a/q| \le q^{-2}$. *Then*

$$S(\alpha) = O\left(n(\log n)^{\frac{9}{2}}\left(q^{-\frac{1}{2}} + (n/q)^{-\frac{1}{2}}\right) + n\exp\left(-\tfrac{1}{2}\sqrt{\log n}\right)\right)$$

Vinogradov

- In 1937 Vinogradov proved the following.

Theorem 1 (Vinogradov 1937)

Let

$$S(\alpha) = \sum_{p \le n} e(\alpha p).$$

Suppose that $q \in \mathbb{N}$, $a \in \mathbb{Z}$, $(q, a) = 1$ *and* $|\alpha - a/q| \le q^{-2}$. *Then*

$$S(\alpha) = O\left(n(\log n)^{\frac{9}{2}}\left(q^{-\frac{1}{2}} + (n/q)^{-\frac{1}{2}}\right) + n\exp\left(-\tfrac{1}{2}\sqrt{\log n}\right)\right)$$

- This gives non-trivial estimates when $(a, q) = 1$ and

$$(\log n)^A < q \le n(\log n)^{-A}, \quad |\alpha - a/q| \le (\log n)^A n^{-1} q^{-1}$$

Vinogradov

- In 1937 Vinogradov proved the following.

Theorem 1 (Vinogradov 1937)

Let

$$S(\alpha) = \sum_{p \le n} e(\alpha p).$$

Suppose that $q \in \mathbb{N}$, $a \in \mathbb{Z}$, $(q, a) = 1$ *and* $|\alpha - a/q| \le q^{-2}$. *Then*

$$S(\alpha) = O\left(n(\log n)^{\frac{9}{2}}\left(q^{-\frac{1}{2}} + (n/q)^{-\frac{1}{2}}\right) + n\exp\left(-\tfrac{1}{2}\sqrt{\log n}\right)\right)$$

- This gives non-trivial estimates when $(a, q) = 1$ and

$$(\log n)^A < q \le n(\log n)^{-A}, \quad |\alpha - a/q| \le (\log n)^A n^{-1} q^{-1}$$

- One can think of these intervals as being “minor arcs”.

Vinogradov

- Thus Vinogradov [1937] was able to establish that if n is odd, then

$$R_3(n) \sim \frac{n^2}{2(\log n)^3}\mathfrak{S}_3(n).$$

Vinogradov

- Thus Vinogradov [1937] was able to establish that if n is odd, then
$$R_3(n) \sim \frac{n^2}{2(\log n)^3}\mathfrak{S}_3(n).$$
- Helfgott has recently refined the method considerably so as to show that
$$R_3(n) > 0 \quad (n > n_0, n \text{ odd})$$
with a decent value for n_0 which apparently enables the $n \le n_0$ to be checked, and so establishes the Goldbach ternary conjecture.

Vinogradov

- Of course the method also gives

$$\sum_{\substack{m=1\\2|m}}^{n} (R_2(m) - \mathrm{li}_2(m)\mathfrak{S}_2(m))^2 \ll n^3(\log n)^{-A}$$

for any fixed positive number A, and consequently

$$E(x) \ll x(\log x)^{-A}.$$

Vinogradov

- Of course the method also gives

$$\sum_{\substack{m=1\\2|m}}^{n} (R_2(m) - \mathrm{li}_2(m)\mathfrak{S}_2(m))^2 \ll n^3(\log n)^{-A}$$

  for any fixed positive number A, and consequently

$$E(x) \ll x(\log x)^{-A}.$$

- Chudakov, van der Corput, Estermann independently [1937].

Vinogradov

- Montgomery and Vaughan [1975] pushed these ideas further and obtained

$$E(x) \ll x^{1-\delta}$$

for some positive number δ.

Vinogradov

- Montgomery and Vaughan [1975] pushed these ideas further and obtained

$$E(x) \ll x^{1-\delta}$$

  for some positive number δ.
- $\delta = \frac{1}{100}$ Jing–Rung Chen and Pan Cheng Dong [1979].

Vinogradov

- Montgomery and Vaughan [1975] pushed these ideas further and obtained

$$E(x) \ll x^{1-\delta}$$

  for some positive number δ.
- $\delta = \frac{1}{100}$ Jing–Rung Chen and Pan Cheng Dong [1979].
- $\delta = 0.121$ Wen Chao Lu [2010]

Vinogradov

- Montgomery and Vaughan [1975] pushed these ideas further and obtained

$$E(x) \ll x^{1-\delta}$$

  for some positive number δ.
- $\delta = \frac{1}{100}$ Jing–Rung Chen and Pan Cheng Dong [1979].
- $\delta = 0.121$ Wen Chao Lu [2010]
- Pintz has claimed $\delta = \frac{1}{3}$.

- We have already seen in homeworks 8,9, 10, the modern version of Vinogradov's theorem

Theorem 2

Let

$$S(\alpha) = \sum_{p \le n} (\log p) e(\alpha p).$$

Suppose that $(q, a) = 1$ *and* $|\alpha - a/q| \le q^{-2}$. *Then*

$$S(\alpha) \ll n(\log n)^{\frac{5}{2}} \left(q^{-1/2} + n^{-1/5} + (n/q)^{-1/2} \right).$$

- Let me now outline the proof of the following theorem.

Theorem 3

We have

$$r_3(n) = \frac{1}{2}\mathfrak{S}_3(n)n^2 + O_A\big(n^2(\log n)^{-A}\big)$$

where

$$\mathfrak{S}_3(n) = \prod_{p\nmid n}\left(1+\frac{1}{(p-1)^3}\right)\prod_{p\mid n}\left(1-\frac{1}{(p-1)^2}\right).$$

- Let me now outline the proof of the following theorem.

Theorem 3

We have

$$r_3(n) = \frac{1}{2}\mathfrak{S}_3(n)n^2 + O_A\big(n^2(\log n)^{-A}\big)$$

where

$$\mathfrak{S}_3(n) = \prod_{p\nmid n}\left(1+\frac{1}{(p-1)^3}\right)\prod_{p\mid n}\left(1-\frac{1}{(p-1)^2}\right).$$

- Let $\mathfrak{U} = (\tau, 1+\tau]$ for some choice of τ, yet to be made. Then

$$r_3(n) = \int_{\mathfrak{U}} S(\alpha)^3 e(-\alpha n)d\alpha.$$

- Let me now outline the proof of the following theorem.

Theorem 3

We have

$$r_3(n) = \frac{1}{2}\mathfrak{S}_3(n)n^2 + O_A\big(n^2(\log n)^{-A}\big)$$

where

$$\mathfrak{S}_3(n) = \prod_{p\nmid n}\left(1+\frac{1}{(p-1)^3}\right)\prod_{p\mid n}\left(1-\frac{1}{(p-1)^2}\right).$$

- Let $\mathfrak{U} = (\tau, 1+\tau]$ for some choice of τ, yet to be made. Then
$$r_3(n) = \int_{\mathfrak{U}} S(\alpha)^3 e(-\alpha n)d\alpha.$$
- We need to have some understanding of how to approximate real numbers α by rational numbers a/q.

Dirchlet

- The next theorem, due to Dirchlet, has a really neat proof.

Theorem 4

Suppose that $Q \geq 1$ *and* $\alpha \in \mathbb{R}$. *There there is a* $q \leq Q$ *and an integer* a *such that* $(q, a) = 1$ *and* $|\alpha - 1/q| \leq \frac{1}{q(1+\lfloor Q \rfloor)}$.

Dirchlet

- The next theorem, due to Dirchlet, has a really neat proof.

Theorem 4

Suppose that $Q \geq 1$ *and* $\alpha \in \mathbb{R}$. *There there is a* $q \leq Q$ *and an integer* a *such that* $(q, a) = 1$ *and* $|\alpha - 1/q| \leq \frac{1}{q(1+\lfloor Q \rfloor)}$.

- *Proof.* Consider the $1 + \lfloor Q \rfloor$ intervals $I_n = \big[(n-1)/(1+\lfloor Q \rfloor), n/(1+\lfloor Q \rfloor)\big)$ with $1 \leq n \leq 1 + \lfloor Q \rfloor$. If there is a $q \leq Q$ such that $\alpha q - \lfloor \alpha q \rfloor \in I_1$, or $\in I_{1+\lfloor Q \rfloor}$, then we are done. Hence we can suppose that at least one of the remaining I_n contains $\alpha q_1 - \lfloor \alpha q_1 \rfloor$ and $\alpha q_2 - \lfloor \alpha q_2 \rfloor$ for some $q_1 \neq q_2$. Then we can take $q = |q_2 - q_1|$.

- When α is close to a rational number a/q with q small, say $\alpha = a/q + \beta$ with β small (whatever that many mean) we can hope to approximate to

$$S(\alpha) = \sum_{p \le n} (\log p) e(\alpha p)$$

by sorting the primes according to residue classes modulo q.

- When α is close to a rational number a/q with q small, say $\alpha = a/q + \beta$ with β small (whatever that many mean) we can hope to approximate to

$$S(\alpha) = \sum_{p \le n} (\log p) e(\alpha p)$$

by sorting the primes according to residue classes modulo q.

- Moreover all but a small number of the primes are in reduced residue classes, so we can expect that

$$S(\alpha) \sim \sum_{\substack{r=1 \\ (r,q)=1}}^{q} e(ar/q) \sum_{\substack{p \le n \\ p \equiv r \pmod q}} (\log p) e(\beta p)$$

$$= \frac{1}{\phi(q)} \sum_{\substack{r=1 \\ (r,q)=1}}^{q} e(ar/q) \sum_{\chi \pmod q} \overline{\chi}(r) \sum_{p \le n} (\log p) \chi(p) e(\beta p)$$

- When α is close to a rational number a/q with q small, say $\alpha = a/q + \beta$ with β small (whatever that many mean) we can hope to approximate to

$$S(\alpha) = \sum_{p \le n} (\log p) e(\alpha p)$$

by sorting the primes according to residue classes modulo q.

- Moreover all but a small number of the primes are in reduced residue classes, so we can expect that

$$S(\alpha) \sim \sum_{\substack{r=1 \\ (r,q)=1}}^{q} e(ar/q) \sum_{\substack{p \le n \\ p \equiv r \pmod q}} (\log p) e(\beta p)$$

$$= \frac{1}{\phi(q)} \sum_{\substack{r=1 \\ (r,q)=1}}^{q} e(ar/q) \sum_{\chi \pmod q} \overline{\chi}(r) \sum_{p \le n} (\log p) \chi(p) e(\beta p)$$

- The error in the first step will be $\ll (\log q) \log n$

- Thus $S(\alpha)$

$$\sim \frac{1}{\phi(q)} \sum_{\substack{r=1\\(r,q)=1}}^{q} e(ar/q) \sum_{\chi \pmod q} \overline{\chi}(r) \sum_{p\le n} (\log p)\chi(p)e(\beta p)$$

$$= \frac{1}{\phi(q)} \sum_{\chi \pmod q} \sum_{\substack{r=1\\(r,q)=1}}^{q} e(ar/q)\overline{\chi}(r) \sum_{p\le n} (\log p)\chi(p)e(\beta p)$$

$$= \frac{1}{\phi(q)} \sum_{\chi \pmod q} \chi(a)\tau(\overline{\chi}) \sum_{p\le n} (\log p)\chi(p)e(\beta p).$$

- Thus $S(\alpha)$

$$\sim \frac{1}{\phi(q)} \sum_{\substack{r=1\\(r,q)=1}}^{q} e(ar/q) \sum_{\chi \pmod q} \overline{\chi}(r) \sum_{p\le n} (\log p)\chi(p)e(\beta p)$$

$$= \frac{1}{\phi(q)} \sum_{\chi \pmod q} \sum_{\substack{r=1\\(r,q)=1}}^{q} e(ar/q)\overline{\chi}(r) \sum_{p\le n} (\log p)\chi(p)e(\beta p)$$

$$= \frac{1}{\phi(q)} \sum_{\chi \pmod q} \chi(a)\tau(\overline{\chi}) \sum_{p\le n} (\log p)\chi(p)e(\beta p).$$

- We might expect, if β is fairly small and $q \le (\log n)^A$, to be able to use the Siegel-Walfisz theorem to replace the last sum by an error term except when χ is the principal character. In that case $\tau(\chi_0) = \mu(q)$.

- Putting it all together we have

Theorem 5

There is a positive constant c such that if $A \geq 1$ is a fixed positive real number, $q \leq (\log n)^A$, $(a, q) = 1$, $\alpha = a/q + \beta$ and $|\beta| \leq (\log n)^A n^{-1}$, then

$$S(\alpha) = \frac{\mu(q)}{\phi(q)} \sum_{m \leq n} e(\beta m) + O_A\left(n \exp\left(-c\sqrt{\log n}\right)\right).$$

- Putting it all together we have

Theorem 5

There is a positive constant c such that if $A \geq 1$ is a fixed positive real number, $q \leq (\log n)^A$, $(a, q) = 1$, $\alpha = a/q + \beta$ and $|\beta| \leq (\log n)^A n^{-1}$, then

$$S(\alpha) = \frac{\mu(q)}{\phi(q)} \sum_{m \leq n} e(\beta m) + O_A\left(n \exp\left(-c\sqrt{\log n}\right)\right).$$

- The only serious detail in the proof is in dealing with

$$\sum_{p \leq n} \chi(p) e(\beta p).$$

- When $\chi \neq \chi_0$ have

$$\sum_{p\le n}\chi(p)e(\beta p) = \sum_{p\le n}\chi(p)\Big(e(\beta n) - \int_p^n 2\pi i\beta e(\beta t)dt\Big)$$
$$= e(\beta n)\vartheta(n;\chi) - \int_2^n \vartheta(t;\chi)2\pi i\beta e(\beta t)dt$$
$$\ll (1+|\beta|n)n\exp\big(-c'\sqrt{\log n}\big).$$

- When $\chi \neq \chi_0$ have

$$\sum_{p\le n}\chi(p)e(\beta p) = \sum_{p\le n}\chi(p)\Big(e(\beta n) - \int_p^n 2\pi i\beta e(\beta t)dt\Big)$$
$$= e(\beta n)\vartheta(n;\chi) - \int_2^n \vartheta(t;\chi)2\pi i\beta e(\beta t)dt$$
$$\ll (1+|\beta|n)n\exp\big(-c'\sqrt{\log n}\big).$$

- When $\chi = \chi_0$ there is a main term to deal with.

- When $\chi \neq \chi_0$ have

$$\sum_{p\le n}\chi(p)e(\beta p) = \sum_{p\le n}\chi(p)\left(e(\beta n) - \int_p^n 2\pi i\beta e(\beta t)dt\right)$$
$$= e(\beta n)\vartheta(n;\chi) - \int_2^n \vartheta(t;\chi)2\pi i\beta e(\beta t)dt$$
$$\ll (1+|\beta|n)n\exp\big(-c'\sqrt{\log n}\big).$$

- When $\chi = \chi_0$ there is a main term to deal with.
- The slickest way is to write

$$\vartheta(t;\chi_0) = \lfloor t\rfloor + O\left(n\exp\big(-c'\sqrt{\log n}\big)\right)$$

and use the fact

$$\lfloor t\rfloor = \sum_{m\le t} 1$$

to invert the above process to give a main term of

$$\sum_{m\le n} e(\beta m).$$

- We now have two kinds of α for which we have information. Hopefully every α is of one kind or the other.

- We now have two kinds of α for which we have information. Hopefully every α is of one kind or the other.
- We define major and minor arcs (well intervals really, but the term "arc" is retained as a form of homage to the original work of Hardy and Littlewood) as follows.

- Given $a, q \in \mathbb{N}$ with $1 \le a \le q \le (\log n)^A$ and $(a, q) = 1$ we define

$$\mathfrak{M}(q, a) = \{\alpha : |\alpha - a/q| \le n^{-1}(\log n)^A\}.$$

In most situations it is more natural to consider shorter intervals $|\alpha - a/q| \le q^{-1}n^{-1}(\log n)^A$, but in the present context the longer intervals lead to some simplifications.

- Given $a, q \in \mathbb{N}$ with $1 \le a \le q \le (\log n)^A$ and $(a, q) = 1$ we define

$$\mathfrak{M}(q, a) = \{\alpha : |\alpha - a/q| \le n^{-1}(\log n)^A\}.$$

  In most situations it is more natural to consider shorter intervals $|\alpha - a/q| \le q^{-1}n^{-1}(\log n)^A$, but in the present context the longer intervals lead to some simplifications.
- These are the major arcs and we take $\mathfrak{M}$ to be their union.

- Given $a, q \in \mathbb{N}$ with $1 \le a \le q \le (\log n)^A$ and $(a, q) = 1$ we define

$$\mathfrak{M}(q, a) = \{\alpha : |\alpha - a/q| \le n^{-1}(\log n)^A\}.$$

  In most situations it is more natural to consider shorter intervals $|\alpha - a/q| \le q^{-1}n^{-1}(\log n)^A$, but in the present context the longer intervals lead to some simplifications.
- These are the major arcs and we take $\mathfrak{M}$ to be their union.
- Now let $\mathfrak{U} = (\tau, 1 + \tau]$ where $\tau = n^{-1}(\log n)^A$ and let $\mathfrak{m} = \mathfrak{U} \setminus \mathfrak{M}$.

- Given $a, q \in \mathbb{N}$ with $1 \le a \le q \le (\log n)^A$ and $(a, q) = 1$ we define

$$\mathfrak{M}(q, a) = \{\alpha : |\alpha - a/q| \le n^{-1}(\log n)^A\}.$$

  In most situations it is more natural to consider shorter intervals $|\alpha - a/q| \le q^{-1}n^{-1}(\log n)^A$, but in the present context the longer intervals lead to some simplifications.
- These are the major arcs and we take $\mathfrak{M}$ to be their union.
- Now let $\mathfrak{U} = (\tau, 1 + \tau]$ where $\tau = n^{-1}(\log n)^A$ and let $\mathfrak{m} = \mathfrak{U} \setminus \mathfrak{M}$.
- By Dirichlet's theorem on diophantine approximation given $\alpha \in \mathfrak{m}$, there are q, a with $(q, a) = 1$, $q \le n(\log n)^{-A}$ and $|\alpha - a/q| \le q^{-1}n^{-1}(\log n)^A$. Moreover, since $\alpha \notin \mathfrak{M}$ we have $q > (\log n)^A$. Hence, by Theorem 2, for $\alpha \in \mathfrak{m}$

$$\begin{aligned} S(\alpha) &\ll n(\log n)^{\frac{5}{2}} \left(q^{-1/2} + n^{-1/5} + (n/q)^{-1/2}\right) \\ &\ll n(\log n)^{(5-A)/2}. \end{aligned}$$

- This together with Parseval and Chebysev's theorem which gives

$$\int_{\mathfrak{U}} |S(\alpha)|^2 d\alpha = \sum_{p \le n} (\log p)^2 \ll n \log n$$

enables us to give a satisfactory treatment to the minor arcs

Theorem 6

We have

$$\int_{\mathfrak{m}} |S(\alpha)|^3 d\alpha \ll n^2 (\log n)^{(7-A)/2}.$$

- This together with Parseval and Chebysev's theorem which gives

$$\int_{\mathfrak{U}} |S(\alpha)|^2 d\alpha = \sum_{p \le n} (\log p)^2 \ll n \log n$$

enables us to give a satisfactory treatment to the minor arcs

Theorem 6

We have

$$\int_{\mathfrak{m}} |S(\alpha)|^3 d\alpha \ll n^2 (\log n)^{(7-A)/2}.$$

- It remains to deal with the major arcs. Generally in applications of the Hardy-Littlewood method the minor arcs are the hard part, the part where some innovation is required to make progress, and this was originally done by Vinogradov. Typically the major arcs are more routine, and here they were essentially treated earlier by Hardy and Littlewood.

- We have seen that if $(q, a) = 1$, $q \le (\log n)^A$ and $\beta = \alpha - a/q$ satisfies $|\beta| \le n^{-1}(\log n)^A$, then

$$S(\alpha) = \frac{\mu(q)}{\phi(q)} T(\beta) + E$$

where

$$T(\beta) = \sum_{m=1}^{n} e(\beta m)$$

and

$$E \ll n \exp\big(-c\sqrt{\log n}\big).$$

- We have seen that if $(q, a) = 1$, $q \le (\log n)^A$ and $\beta = \alpha - a/q$ satisfies $|\beta| \le n^{-1}(\log n)^A$, then

$$S(\alpha) = \frac{\mu(q)}{\phi(q)} T(\beta) + E$$

where

$$T(\beta) = \sum_{m=1}^{n} e(\beta m)$$

and

$$E \ll n \exp\big(-c\sqrt{\log n}\big).$$

- Then as $|T(\beta)| \le n$ we have

$$S(\alpha)^3 = \frac{\mu(q)}{\phi(q)^3} T(\beta)^3 + O\left(n^3 \exp\big(-c\sqrt{\log n}\big)\right)$$

- We have

$$S(\alpha)^3 = \frac{\mu(q)}{\phi(q)^3} T(\beta)^3 + O\left(n^3 \exp\left(-c\sqrt{\log n}\right)\right)$$

- We have

$$S(\alpha)^3 = \frac{\mu(q)}{\phi(q)^3} T(\beta)^3 + O\left(n^3 \exp\left(-c\sqrt{\log n}\right)\right)$$

- Integrating over $\mathfrak{M}(q,a)$ and summing over a,

$$\sum_{\substack{a=1\\(a,q)=1}}^{q} \int_{\mathfrak{M}(q,a)} S(\alpha)^3 e(-\alpha n)\,d\alpha$$

$$= \frac{\mu(q)c_q(n)}{\phi(q)^3} \int_{-(\log n)^A n^{-1}}^{(\log n)^A n^{-1}} T(\beta)^3 e(-\beta n)\,d\beta$$

$$+ O\left(\phi(q)(\log n)^A n^2 \exp\left(-c\sqrt{\log n}\right)\right).$$

- We have

$$S(\alpha)^3 = \frac{\mu(q)}{\phi(q)^3} T(\beta)^3 + O\left(n^3 \exp\left(-c\sqrt{\log n}\right)\right)$$

- Integrating over $\mathfrak{M}(q,a)$ and summing over a,

$$\sum_{\substack{a=1\\(a,q)=1}}^{q} \int_{\mathfrak{M}(q,a)} S(\alpha)^3 e(-\alpha n)\,d\alpha$$

$$= \frac{\mu(q)c_q(n)}{\phi(q)^3} \int_{-(\log n)^A n^{-1}}^{(\log n)^A n^{-1}} T(\beta)^3 e(-\beta n)\,d\beta$$

$$+ O\left(\phi(q)(\log n)^A n^2 \exp\left(-c\sqrt{\log n}\right)\right).$$

- Observe that the main term has factored into two independent pieces, a local, or "q-adic" piece, and a piece which, in some sense, corresponds to $\mathbb{R}$. $c_q(n)$ is the Ramanujan sum which we studied in homework 3.

- We now sum over the $q \le (\log n)^A$,

$$\sum_{\substack{a=1\\(a,q)=1}}^{q} \int_{\mathfrak{M}(q,a)} S(\alpha)^3 e(-\alpha n)\,d\alpha$$

$$= \frac{\mu(q)c_q(n)}{\phi(q)^3} \int_{-(\log n)^A n^{-1}}^{(\log n)^A n^{-1}} T(\beta)^3 e(-\beta n)\,d\beta$$

$$+ O\Big(\phi(q)(\log n)^A n^2 \exp\big(-c\sqrt{\log n}\big)\Big)$$

- We now sum over the $q \le (\log n)^A$,

$$\sum_{\substack{a=1\\(a,q)=1}}^{q} \int_{\mathfrak{M}(q,a)} S(\alpha)^3 e(-\alpha n)\,d\alpha$$

$$= \frac{\mu(q)c_q(n)}{\phi(q)^3} \int_{-(\log n)^A n^{-1}}^{(\log n)^A n^{-1}} T(\beta)^3 e(-\beta n)\,d\beta$$

$$+ O\Big(\phi(q)(\log n)^A n^2 \exp\big(-c\sqrt{\log n}\big)\Big)$$

- Thus $\displaystyle\int_{\mathfrak{M}} S(\alpha)^3 e(-\alpha n)\,d\alpha$

$$= \mathfrak{S}\big(n, (\log n)^A\big) J(n) + O\Big((\log n)^{3A} n^2 \exp\big(-c\sqrt{\log n}\big)\Big)$$

where

$$\mathfrak{S}(n, Q) = \sum_{q \le Q} \mu(q) c_q(n) \phi(q)^{-3},$$

$$J(n) = \int_{-(\log n)^A n^{-1}}^{(\log n)^A n^{-1}} T(\beta)^3 e(-\beta n)\,d\beta$$

- Thus $\displaystyle\int_{\mathfrak{M}} S(\alpha)^3 e(-\alpha n)\,d\alpha$

$$= \mathfrak{S}\big(n, (\log n)^A\big) J(n) + O\Big(n^2 \exp\big(-c'\sqrt{\log n}\big)\Big)$$

$$\mathfrak{S}(n, Q) = \sum_{q \le Q} \mu(q) c_q(n) \phi(q)^{-3},$$

$$J(n) = \int_{-(\log n)^A n^{-1}}^{(\log n)^A n^{-1}} T(\beta)^3 e(-\beta n)\,d\beta$$

- Thus $\displaystyle\int_{\mathfrak{M}} S(\alpha)^3 e(-\alpha n)d\alpha$

$$= \mathfrak{S}\big(n, (\log n)^A\big) J(n) + O\Big(n^2 \exp\big(-c'\sqrt{\log n}\big)\Big)$$

$$\mathfrak{S}(n, Q) = \sum_{q \le Q} \mu(q) c_q(n) \phi(q)^{-3},$$

$$J(n) = \int_{-(\log n)^A n^{-1}}^{(\log n)^A n^{-1}} T(\beta)^3 e(-\beta n)d\beta$$

- The sum $T(\beta) = \sum_{m=1}^{n} e(\beta n)$ satisfies $T(\beta) \ll \|\beta\|^{-1}$.

- Thus $\displaystyle\int_{\mathfrak{M}} S(\alpha)^3 e(-\alpha n)d\alpha$

$$= \mathfrak{S}\big(n,(\log n)^A\big)J(n) + O\Big(n^2\exp\big(-c'\sqrt{\log n}\big)\Big)$$

$$\mathfrak{S}(n,Q) = \sum_{q\le Q}\mu(q)c_q(n)\phi(q)^{-3},$$

$$J(n) = \int_{-(\log n)^A n^{-1}}^{(\log n)^A n^{-1}} T(\beta)^3 e(-\beta n)d\beta$$

- The sum $T(\beta) = \sum_{m=1}^{n} e(\beta n)$ satisfies $T(\beta) \ll \|\beta\|^{-1}$.
- Thus

$$\int_{(\log n)^A n^{-1}\le|\beta|\le 1/2} |T(\beta)|^3 d\beta$$

$$\ll \int_{(\log n)^A n^{-1}}^{1/2} \beta^{-3}d\beta \ll n^2(\log n)^{-2A}.$$

- We have just shown that

$$J(n) = \int_{-1/2}^{1/2} T(\beta)^3 e(-\beta n) d\beta + O\big((\log n)^{-2A} n^2\big)$$

- We have just shown that

$$J(n) = \int_{-1/2}^{1/2} T(\beta)^3 e(-\beta n) d\beta + O\big((\log n)^{-2A} n^2\big)$$

- The integral here simply the number N of choices of m_j so that $m_1 + m_2 + m_3 = n$.

- We have just shown that

$$J(n) = \int_{-1/2}^{1/2} T(\beta)^3 e(-\beta n) d\beta + O\big((\log n)^{-2A} n^2\big)$$

- The integral here simply the number N of choices of m_j so that $m_1 + m_2 + m_3 = n$.
- Since the number of choices of m_1, m_2 with $m_1 + m_2 = l$ is $l - 1$ it follows that

$$N = \sum_{1 \le m_3 \le n-2} (n - 1 - m_3) = \frac{1}{2}(n-1)(n-2).$$

- We have just shown that

$$J(n) = \int_{-1/2}^{1/2} T(\beta)^3 e(-\beta n) d\beta + O\big((\log n)^{-2A} n^2\big)$$

- The integral here simply the number N of choices of m_j so that $m_1 + m_2 + m_3 = n$.
- Since the number of choices of m_1, m_2 with $m_1 + m_2 = l$ is $l - 1$ it follows that

$$N = \sum_{1 \le m_3 \le n-2} (n - 1 - m_3) = \frac{1}{2}(n-1)(n-2).$$

- Hence

$$J(n) = \frac{1}{2} n^2 + O\big((\log n)^{-2A} n^2\big).$$

- We now have to deal with $\mathfrak{S}(n, Q)$.

- We have

$$\mathfrak{S}(n, Q) = \sum_{q \le Q} \mu(q) c_q(n) \phi(q)^{-3},$$

with $Q = (\log n)^A$.

- We have

$$\mathfrak{S}(n,Q)=\sum_{q\le Q}\mu(q)c_q(n)\phi(q)^{-3},$$

with $Q=(\log n)^A$.

- Trivially $|c_q(n)|\le\phi(q)$ so

$$\sum_{q>Q}\mu(q)c_q(n)\phi(q)^{-3}\ll\sum_{q>Q}\mu(q)^2\phi(q)^{-2}$$

$$\ll Q^{-1/2}\sum_{q=1}^{\infty}\mu(q)^2q^{1/2}\phi(q)^{-2}.$$

- We have

$$\mathfrak{S}(n,Q)=\sum_{q\le Q}\mu(q)c_q(n)\phi(q)^{-3},$$

with $Q=(\log n)^A$.

- Trivially $|c_q(n)|\le\phi(q)$ so

$$\sum_{q>Q}\mu(q)c_q(n)\phi(q)^{-3}\ll\sum_{q>Q}\mu(q)^2\phi(q)^{-2}$$

$$\ll Q^{-1/2}\sum_{q=1}^{\infty}\mu(q)^2q^{1/2}\phi(q)^{-2}.$$

- Here the infinite series has the absolutely convergent Euler product $\prod_p\left(1+\dfrac{p^{1/2}}{(p-1)^2}\right)$.

- We have
$$\mathfrak{S}(n,Q)=\sum_{q\le Q}\mu(q)c_q(n)\phi(q)^{-3},$$
with $Q=(\log n)^A$.
- Trivially $|c_q(n)|\le\phi(q)$ so
$$\sum_{q>Q}\mu(q)c_q(n)\phi(q)^{-3}\ll\sum_{q>Q}\mu(q)^2\phi(q)^{-2}$$
$$\ll Q^{-1/2}\sum_{q=1}^{\infty}\mu(q)^2q^{1/2}\phi(q)^{-2}.$$
- Here the infinite series has the absolutely convergent Euler product $\prod_p\left(1+\frac{p^{1/2}}{(p-1)^2}\right)$.
- Thus $\mathfrak{S}(n,Q)=\mathfrak{S}(n)+O(Q^{-1/2})$ where $\mathfrak{S}(n)=$
$$\sum_{q=1}^{\infty}\frac{\mu(q)c_q(n)}{\phi(q)^3}=\prod_{p\nmid n}\left(1+\frac{1}{(p-1)^3}\right)\prod_{p\mid n}\left(1-\frac{1}{(p-1)^2}\right)$$

- Putting it all together we have established the following theorem.

Theorem 7

For every fixed $B \geq 1$ and every odd n we have

$$\sum_{\substack{p_1,p_2,p_3\\ p_1+p_2+p_3=n}} (\log p_1)\log p_2)(\log p_3) = \frac{n^2}{2}\mathfrak{S}(n) + O_B\left(n^2(\log n)^{-B}\right)$$

where

$$\begin{aligned}\mathfrak{S}(n) &= \sum_{q=1}^{\infty} \mu(q)c_q(n)\phi(q)^{-3}\\ &= \prod_{p\nmid n}\left(1+\frac{1}{(p-1)^3}\right)\prod_{p\mid n}\left(1-\frac{1}{(p-1)^2}\right).\end{aligned}$$

- Another theorem which can be proved by the method.

Theorem 8

For every fixed $B \geq 1$ and every n we have

$$\sum_{m=1}^{n} |r_2(m) - m\mathfrak{S}_2(m)|^2 \ll n^3(\log n)^{-B}$$

where $r_2(m) = \sum_{\substack{p_1,p_2 \\ p_1+p_2=m}} (\log p_1)\log p_2)$, $\mathfrak{S}_2(m) =$

$$\prod_{p\nmid m}\left(\frac{p(p-2)}{(p-1)^2}\right)\prod_{p|m}\frac{p}{(p-1)}.$$

- Another theorem which can be proved by the method.

Theorem 8

For every fixed $B \geq 1$ and every n we have

$$\sum_{m=1}^{n} |r_2(m) - m\mathfrak{S}_2(m)|^2 \ll n^3(logn)^{-B}$$

where $r_2(m) = \sum_{\substack{p_1,p_2 \\ p_1+p_2=m}} (\log p_1)\log p_2)$, $\mathfrak{S}_2(m) =$

$$\prod_{p\nmid m}\left(\frac{p(p-2)}{(p-1)^2}\right)\prod_{p|m}\frac{p}{(p-1)}.$$

- Note that any terms with m odd contribute $\ll n\log n$.

- Another theorem which can be proved by the method.

Theorem 8

For every fixed $B \geq 1$ and every n we have

$$\sum_{m=1}^{n} |r_2(m) - m\mathfrak{S}_2(m)|^2 \ll n^3(\log n)^{-B}$$

where $r_2(m) = \sum_{\substack{p_1,p_2 \\ p_1+p_2=m}} (\log p_1)\log p_2)$, $\mathfrak{S}_2(m) =$

$$\prod_{p\nmid m}\left(\frac{p(p-2)}{(p-1)^2}\right)\prod_{p|m}\frac{p}{(p-1)}.$$

- Note that any terms with m odd contribute $\ll n\log n$.
- Consequently we have

Corollary 9

For every fixed $B \geq 1$
$\mathrm{card}\{m \leq n : 2|m, m \neq p_1 + p_2\} \ll_B n(\log n)^{-B}$.

$$\sum_{\substack{m=1\\2|m}}^{n} |r_2(m) - m\mathfrak{S}_2(m)|^2 \ll n^3(logn)^{-B},$$

$$\mathfrak{S}_2(m) = \prod_{p\nmid m}\left(\frac{p(p-2)}{(p-1)^2}\right)\prod_{p|m}\frac{p}{(p-1)}$$

- To prove $\text{card}\{m \le n : 2|m, m \ne p_1 + p_2\} \ll_B n(\log n)^{-B}$ note that for $2|m$ we have

$$\mathfrak{S}_2(m) \gg 1$$

$$\sum_{\substack{m=1\\2|m}}^{n} |r_2(m) - m\mathfrak{S}_2(m)|^2 \ll n^3(logn)^{-B},$$

$$\mathfrak{S}_2(m) = \prod_{p\nmid m}\left(\frac{p(p-2)}{(p-1)^2}\right)\prod_{p|m}\frac{p}{(p-1)}$$

- To prove $\text{card}\{m \le n : 2|m, m \ne p_1 + p_2\} \ll_B n(\log n)^{-B}$ note that for $2|m$ we have

$$\mathfrak{S}_2(m) \gg 1$$

- Thus

$$n^2\,\text{card}\{n/2 < m \le n : 2|m, m \ne p_1 + p_2\} \ll \sum_{\substack{m=1\\2|m}}^{n} |r_2(m) - m\mathfrak{S}_2(m)|^2$$

$$\sum_{\substack{m=1\\2|m}}^{n} |r_2(m) - m\mathfrak{S}_2(m)|^2 \ll n^3(logn)^{-B},$$

$$\mathfrak{S}_2(m) = \prod_{p\nmid m}\left(\frac{p(p-2)}{(p-1)^2}\right)\prod_{p|m}\frac{p}{(p-1)}$$

- To prove $\text{card}\{m \le n : 2|m, m \ne p_1 + p_2\} \ll_B n(\log n)^{-B}$ note that for $2|m$ we have

$$\mathfrak{S}_2(m) \gg 1$$

- Thus

$$n^2\,\text{card}\{n/2 < m \le n : 2|m, m \ne p_1 + p_2\} \ll \sum_{\substack{m=1\\2|m}}^{n} |r_2(m) - m\mathfrak{S}_2(m)|^2$$

- Replace n by $\lfloor n2^{-k}\rfloor$ and sum over k

Proof of Theorem 8

- We have

$$r_2(m) = R_{\mathfrak{M}}(m) + R_{\mathfrak{m}}(m)$$

where

$$R_{\mathfrak{B}}(m) = \int_{\mathfrak{B}} S(\alpha)^2 e(-\alpha m) d\alpha.$$

Proof of Theorem 8

- We have

$$r_2(m) = R_{\mathfrak{M}}(m) + R_{\mathfrak{m}}(m)$$

where

$$R_{\mathfrak{B}}(m) = \int_{\mathfrak{B}} S(\alpha)^2 e(-\alpha m) d\alpha.$$

- By Bessel's inequality

$$\sum_m |R_{\mathfrak{m}}(m)|^2 \le \int_{\mathfrak{m}} |S(\alpha)|^4 d\alpha \ll n^3 (\log n)^{6-A},$$

Proof of Theorem 8

- We have
$$r_2(m) = R_{\mathfrak{M}}(m) + R_{\mathfrak{m}}(m)$$
where
$$R_{\mathfrak{B}}(m) = \int_{\mathfrak{B}} S(\alpha)^2 e(-\alpha m) d\alpha.$$
- By Bessel's inequality
$$\sum_m |R_{\mathfrak{m}}(m)|^2 \le \int_{\mathfrak{m}} |S(\alpha)|^4 d\alpha \ll n^3 (\log n)^{6-A},$$
- so we can concentrate on
$$\sum_{m=1}^{n} |R_{\mathfrak{M}}(m) - m\mathfrak{S}_2(m)|^2,$$
so just another tricky endgame.

- As in the ternary case, for $\alpha \in \mathfrak{M}(q, a)$ we have

$$S(\alpha)^2 = \frac{\mu(q)^2}{\phi(q)^2} T(\beta)^2 + O\left(n^2 \exp(-c\sqrt{\log n})\right)$$

- As in the ternary case, for $\alpha \in \mathfrak{M}(q,a)$ we have

$$S(\alpha)^2 = \frac{\mu(q)^2}{\phi(q)^2} T(\beta)^2 + O\left(n^2 \exp(-c\sqrt{\log n})\right)$$

- Thus $R_{\mathfrak{M}}(m) = \int_{\mathfrak{M}} S(\alpha)^2 e(-\alpha m) d\alpha =$

$$\mathfrak{S}_2\left(m, (\log n)^A\right) J_2(m) + O\left((\log n)^{3A} n^2 \exp\left(-c\sqrt{\log n}\right)\right)$$

where

$$\mathfrak{S}_2(m,Q) = \sum_{q \le Q} \mu(q)^2 c_q(m) \phi(q)^{-2},$$

$$J_2(n) = \int_{-(\log n)^A n^{-1}}^{(\log n)^A n^{-1}} T(\beta)^2 e(-\beta m) d\beta$$

$$R_{\mathfrak{M}}(m) = \mathfrak{S}_2\big(m, (\log n)^A\big) J_2(m) + O\Big(n^2 \exp\big(-c'\sqrt{\log n}\big)\Big),$$

$$\mathfrak{S}_2(m, Q) = \sum_{q \le Q} \frac{\mu(q)^2}{\phi(q)^2} c_q(m),$$

$$J_2(m) = \int_{-(\log n)^A n^{-1}}^{(\log n)^A n^{-1}} T(\beta)^2 e(-\beta m) d\beta.$$

- We have $J_2(m) = \displaystyle\int_{-\frac{1}{2}}^{\frac{1}{2}} T(\beta)^2 e(-\beta m) d\beta + O\big(n(\log n)^{-A}\big)$

$$R_{\mathfrak{M}}(m) = \mathfrak{S}_2\big(m, (\log n)^A\big) J_2(m) + O\Big(n^2 \exp\big(-c'\sqrt{\log n}\big)\Big),$$

$$\mathfrak{S}_2(m, Q) = \sum_{q \le Q} \frac{\mu(q)^2}{\phi(q)^2} c_q(m),$$

$$J_2(m) = \int_{-(\log n)^A n^{-1}}^{(\log n)^A n^{-1}} T(\beta)^2 e(-\beta m) d\beta.$$

- We have $J_2(m) = \displaystyle\int_{-\frac{1}{2}}^{\frac{1}{2}} T(\beta)^2 e(-\beta m) d\beta + O\big(n(\log n)^{-A}\big)$
- and $\mathfrak{S}_2(m, Q) \ll \displaystyle\sum_{q \le Q} \mu(q)^2 \phi(q)^{-1} \ll \log Q.$

$$R_{\mathfrak{M}}(m) = \mathfrak{S}_2\big(m, (\log n)^A\big) J_2(m) + O\Big(n^2 \exp\big(-c'\sqrt{\log n}\big)\Big),$$

$$\mathfrak{S}_2(m, Q) = \sum_{q \le Q} \frac{\mu(q)^2}{\phi(q)^2} c_q(m),$$

$$J_2(m) = \int_{-(\log n)^A n^{-1}}^{(\log n)^A n^{-1}} T(\beta)^2 e(-\beta m) d\beta.$$

- We have $J_2(m) = \displaystyle\int_{-\frac{1}{2}}^{\frac{1}{2}} T(\beta)^2 e(-\beta m) d\beta + O\big(n(\log n)^{-A}\big)$
- and $\mathfrak{S}_2(m, Q) \ll \displaystyle\sum_{q \le Q} \mu(q)^2 \phi(q)^{-1} \ll \log Q.$
- If $m \le n$, the integral is $m - 1$, so

$$\sum_{m=1}^{n} |R_{\mathfrak{M}}(m) - m\mathfrak{S}_2(m)|^2$$

$$\ll \sum_{m=1}^{n} \Big|m\mathfrak{S}_2(m, \log^A n) - m\mathfrak{S}_2(m)\Big|^2 + n^3(\log n)^{-2A}.$$

$$\sum_{m=1}^{n} |R_{\mathfrak{M}}(m) - m\mathfrak{S}_2(m)|^2$$

$$\ll \sum_{m=1}^{n} \left| m\mathfrak{S}_2(m, \log^A n) - m\mathfrak{S}_2(m) \right|^2 + n^3(\log n)^{-2A}.$$

- This is a tricky because we have to use the cancellation in $c_q(m)$. We can try $c_q(m) = \sum_{r|(q,m)} r\mu(q/r)$ and this gives

$$\sum_{m=1}^{n} |R_{\mathfrak{M}}(m) - m\mathfrak{S}_2(m)|^2$$

$$\ll \sum_{m=1}^{n} \left| m\mathfrak{S}_2(m, \log^A n) - m\mathfrak{S}_2(m) \right|^2 + n^3 (\log n)^{-2A}.$$

- This is a tricky because we have to use the cancellation in $c_q(m)$. We can try $c_q(m) = \sum_{r|(q,m)} r\mu(q/r)$ and this gives
-

$$\sum_{Q<q\le R} \frac{\mu(q)^2}{\phi(q)^2} c_q(m) = \sum_{r|m} \frac{r}{\phi(2)^2} \sum_{Q/r<s\le R/s} \frac{\mu(rs)^2\mu(s)}{\phi(s)^2}.$$

$$\sum_{m=1}^{n} |R_{\mathfrak{M}}(m) - m\mathfrak{S}_2(m)|^2$$

$$\ll \sum_{m=1}^{n} \left| m\mathfrak{S}_2(m, \log^A n) - m\mathfrak{S}_2(m) \right|^2 + n^3(\log n)^{-2A}.$$

- This is a tricky because we have to use the cancellation in $c_q(m)$. We can try $c_q(m) = \sum_{r|(q,m)} r\mu(q/r)$ and this gives
- $$\sum_{Q<q\le R} \frac{\mu(q)^2}{\phi(q)^2} c_q(m) = \sum_{r|m} \frac{r}{\phi(2)^2} \sum_{Q/r<s\le R/s} \frac{\mu(rs)^2\mu(s)}{\phi(s)^2}.$$
- The sum over s converges nicely so we are left to bound
$$\sum_{r|m} \frac{r}{\phi(r)^2} \min(1, r/Q)$$

$$\sum_{m=1}^{n} |R_{\mathfrak{M}}(m) - m\mathfrak{S}_2(m)|^2$$

$$\ll \sum_{m=1}^{n} \left| m\mathfrak{S}_2(m, \log^A n) - m\mathfrak{S}_2(m) \right|^2 + n^3 (\log n)^{-2A}.$$

- This is a tricky because we have to use the cancellation in $c_q(m)$. We can try $c_q(m) = \sum_{r|(q,m)} r\mu(q/r)$ and this gives
- $$\sum_{Q<q\le R} \frac{\mu(q)^2}{\phi(q)^2} c_q(m) = \sum_{r|m} \frac{r}{\phi(2)^2} \sum_{Q/r<s\le R/s} \frac{\mu(rs)^2\mu(s)}{\phi(s)^2}.$$
- The sum over s converges nicely so we are left to bound
$$\sum_{r|m} \frac{r}{\phi(r)^2} \min(1, r/Q)$$
- We would want to apply this when $Q = (\log n)^A$, but unfortunately there are $m \le n$ for which $d(m)$ is substantially larger than this.

$$\sum_{m=1}^{n} |R_{\mathfrak{M}}(m) - m\mathfrak{S}_2(m)|^2$$

$$\ll n^2 \sum_{m=1}^{n} \left| \sum_{q>\log^A n} \frac{\mu(q)^2}{\phi(q)^2} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} e(am/q) \right|^2 + n^3(\log n)^{-2A}.$$

- When $Q \le R < R' \le 2R$ by the dual of the large sieve

$$\sum_{m=1}^{n} \left| \sum_{R<q\le R'} \frac{\mu(q)^2}{\phi(q)^2} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} e(am/q) \right|^2$$

$$\ll (n + R^{-2}) \sum_{R<q\le R'} \phi(q) \frac{\mu(q)^4}{\phi(q)^4} \ll nR^{-2} + 1.$$

$$\sum_{m=1}^{n} |R_{\mathfrak{M}}(m) - m\mathfrak{S}_2(m)|^2$$

$$\ll n^2 \sum_{m=1}^{n} \left| \sum_{q>\log^A n} \frac{\mu(q)^2}{\phi(q)^2} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} e(am/q) \right|^2 + n^3(\log n)^{-2A}.$$

- When $Q \le R < R' \le 2R$ by the dual of the large sieve

$$\sum_{m=1}^{n} \left| \sum_{R<q\le R'} \frac{\mu(q)^2}{\phi(q)^2} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} e(am/q) \right|^2$$

$$\ll (n + R^{-2}) \sum_{R<q\le R'} \phi(q) \frac{\mu(q)^4}{\phi(q)^4} \ll nR^{-2} + 1.$$

- Thus $(\log n)^A < q \le n$ contributes $\ll n(\log n)^{2-2A}$.

$$\sum_{m=1}^{n} |R_{\mathfrak{M}}(m) - m\mathfrak{S}_2(m)|^2$$

$$\ll n^2 \sum_{m=1}^{n} \left| \sum_{q>\log^A n} \frac{\mu(q)^2}{\phi(q)^2} \sum_{\substack{a=1\\(a,q)=1}}^{q} e(am/q) \right|^2 + n^3(\log n)^{-2A}.$$

- When $Q \le R < R' \le 2R$ by the dual of the large sieve

$$\sum_{m=1}^{n} \left| \sum_{R<q\le R'} \frac{\mu(q)^2}{\phi(q)^2} \sum_{\substack{a=1\\(a,q)=1}}^{q} e(am/q) \right|^2$$

$$\ll (n + R^{-2}) \sum_{R<q\le R'} \phi(q) \frac{\mu(q)^4}{\phi(q)^4} \ll nR^{-2} + 1.$$

- Thus $(\log n)^A < q \le n$ contributes $\ll n(\log n)^{2-2A}$.
- For the $q > n$ we can use $\sum_{r|m} \frac{r}{\phi(r)^2} \min(1, r/n) \ll n^{-1/2}$.

- Vinogradov and Hua [1965] extended the method to

$$\sum_{p\le X} e(\alpha p^k)$$

- Vinogradov and Hua [1965] extended the method to

$$\sum_{p \le X} e(\alpha p^k)$$

- There is a large body of work on the solubility of

$$p_1^k + \cdots + p_s^k = n.$$

- Vinogradov and Hua [1965] extended the method to

$$\sum_{p \le X} e(\alpha p^k)$$

- There is a large body of work on the solubility of

$$p_1^k + \cdots + p_s^k = n.$$

- There are also many rather different applications. Vinogradov [1938] obtains non–trivial bounds for

$$\sum_{p \le x} \chi(p + a) \quad \chi \ne \chi_0 \mod q.$$

See Friedlander, Gong and Shparlinski [2010].

Vinogradov

- Another application of Vinogradov's method, due to Piatetski–Shapiro [1953] states that when $1 \le c \le \frac{12}{11}$,

$$\operatorname{card}\{n \le x : \lfloor n^c \rfloor \text{ prime}\} \sim \frac{x}{c \log x}.$$

Vinogradov

- Another application of Vinogradov's method, due to Piatetski–Shapiro [1953] states that when $1 \le c \le \frac{12}{11}$,

$$\operatorname{card}\{n \le x : \lfloor n^c \rfloor \text{ prime}\} \sim \frac{x}{c \log x}.$$

- There are quite a number of papers increasing the upper bound for c. The best that I have seen is

$$1 \le c < \frac{243}{205} = 1.18\ldots$$

due to Rivat and Wu [2001]

Hardy and Littlewoood

- The Hardy–Littlewood method is quite effective for ternary problems, but much less so for binary problems.

Hardy and Littlewoood

- The Hardy–Littlewood method is quite effective for ternary problems, but much less so for binary problems.
- However it has been quite successful in creating conjectures. The procedure is quite simple. One assumes without proof that the arcs one cannot handle, the "minor arcs", make a negligible contribution! In this way they were able to write down a large class of plausible conjectures.

Hardy and Littlewoood

- The Hardy–Littlewood method is quite effective for ternary problems, but much less so for binary problems.
- However it has been quite successful in creating conjectures. The procedure is quite simple. One assumes without proof that the arcs one cannot handle, the "minor arcs", make a negligible contribution! In this way they were able to write down a large class of plausible conjectures.
- One such is the following. Let

$$\psi_{2k}(x) = \sum_{2k<n\le x} \Lambda(n)\Lambda(n-2k).$$

Then

$$\psi_{2k}(x) \sim x\mathfrak{S}_2(2k) \quad \text{as } x \to \infty$$

Hardy and Littlewoood

- Whilst this seems well out of reach, Lavrik [1960] (van der Corput [1937] had earlier shown something similar but with the sum over n replaced by a sum restricted to primes p for which $p-2k$ is also prime) has shown that

$$\sum_{k\le x/2}(\psi_{2k}(x)-(x-2k)\mathfrak{S}_2(2k))^2\ll x^3(\log x)^{-A}.$$

Hardy and Littlewoood

- Whilst this seems well out of reach, Lavrik [1960] (van der Corput [1937] had earlier shown something similar but with the sum over n replaced by a sum restricted to primes p for which $p-2k$ is also prime) has shown that

$$\sum_{k\le x/2}(\psi_{2k}(x)-(x-2k)\mathfrak{S}_2(2k))^2\ll x^3(\log x)^{-A}.$$

- We shall see later that this has its uses.

Hardy and Littlewood

- Another of the Hardy and Littlewood conjectures concerns k–tuples of primes. Suppose that $\mathbf{h} = h_1, \dots, h_k$ and let $\nu(q) = \nu(q; \mathbf{h})$ be the number of distinct residue classes modulo q amongst the $\mathbf{h}$. Let

$$\pi_k(x; \mathbf{h}) = \operatorname{card}\{n \le x : n + h_1, \dots, n + h_k \text{ all prime}\}$$

and suppose that for every $q \in \mathbb{N}$ we have $\nu(q) < q$. Then

$$\pi_k(x; \mathbf{h}) \sim \frac{x}{(\log x)^k} \mathfrak{S}_k(\mathbf{h})$$

where $\mathfrak{S}_k(\mathbf{h}) = \left(\prod_{p \nmid \Delta} \frac{p^k - kp^{k-1}}{(p-1)^k} \right) \prod_{p \mid \Delta} \frac{p^k - \nu(p)p^{k-1}}{(p-1)^k}$

and $\Delta = \prod_{1 \le i < j \le k} |h_i - h_j|$.