GOLDBACH'S PROBLEMS

ALEX RICE

Abstract. These are notes from the UGA Analysis and Arithmetic Combinatorics Learning Seminar from Fall 2009, organized by John Doyle, Neil Lyall, and Alex Rice.

In these notes, we introduce Vinogradov's Three Primes Theorem, the solution to the ternary Goldbach Problem and an application of the Hardy-Littlewood Circle Method. We first state the result in its most accessible, least quantitative form, and then introduce the more quantitative version, encapsulated by an asymptotic formula for the three-fold convolution of the von Mangoldt function. Next, we begin the meat of the circle method by defining the major arcs, and giving an estimate on their complement, conditioned on a powerful analog of the Weyl Inequality due to Vinogradov himself. We then give an estimate on the major arcs that provides the main term in the asymptotic formula and proves the result, provided we take Vinogradov's minor arc estimate and a theorem of Siegel and Walfisz on faith.

Secondly, we utilize many of the same lemmas and estimates from the proof of Vinogradov's Theorem to obtain a partial result of the more well-known binary Goldbach Conjecture.

1. Vinogradov's Three Primes Theorem

Theorem 1 (Vinogradov, 1937)**.** *Every sufficiently large odd integer can be written as the sum of three primes.*

This phrasing of the result is perhaps the most satisfying, but in truth, the full result is far more quantitative, and gives an order of growth for the number of representations of an odd integer as the sum of three primes. We begin with the definition of the quantity in question, and a discussion of intuition for its approximate size.

Definition. Let $\mathcal{P}$ denote the primes. For $N \in \mathbb{N}$, we define

$$r(N) = \#\{(p_1, p_2, p_3) \in \mathcal{P}_N^3 : p_1 + p_2 + p_3 = N\},$$

where $\mathcal{P}_N = \mathcal{P} \cap [1, N]$.

How big would we expect $r(N)$ to be? We know from the prime number theorem that $|\mathcal{P}_N| \sim \frac{N}{\log N}$, so $|\mathcal{P}_N^3| \sim \frac{N^3}{\log^3 N}$. Of course, for $(p_1, p_2, p_3) \in \mathcal{P}_N^3$, we have that $p_1 + p_2 + p_3 \in \{1, 2, \dots, 3N\}$, so if we assume that these sums are more or less "uniformly distributed" (quite the assumption), then we would expect $r(N) \sim \frac{N^3}{\log^3 N} \cdot \frac{1}{3N} \sim \frac{N^2}{\log^3 N}$. In fact, we will show that there exist $C > 0$ and $N_0 \in \mathbb{N}$ such that $r(N) \geq C\frac{N^2}{\log^3 N}$ for all $N \geq N_0$. We begin our attack, much like in our discussion of Waring's problem, by using orthogonality and phrasing the question more analytically.

Definition. For $f\colon \mathbb{N} \to \mathbb{C}$, we define $f^*\colon \mathbb{N} \to \mathbb{C}$ by

$$f^*(N) = \sum_{k_1+k_2+k_3=N} f(k_1)f(k_2)f(k_3) = \int_0^1 (\widehat{f}_N(\alpha))^3 e^{2\pi i N\alpha} d\alpha,$$

where $\widehat{f}_N(\alpha) = \sum_{k=1}^{N} f(k)e^{-2\pi i k\alpha}$.

The first equality defines the notation, while the second equality follows from the orthogonality relation

$$\int_0^1 e^{2\pi i k\alpha} d\alpha = \begin{cases} 1 & \text{if } k = 0 \\ 0 & \text{else} \end{cases}.$$

We notice that f^* is non-negative real-valued as long as f is, and we also see that $1^*_{\mathcal{P}}(N) = r(N)$, but it will be beneficial for us to utilize slightly modified functions in place of $1_{\mathcal{P}}$.

Definition. We define $g, \Lambda\colon \mathbb{N} \to [0,\infty)$ by

$$g(n) = \begin{cases} \log p, & \text{if } n = p \in \mathcal{P} \\ 0, & \text{else} \end{cases}, \Lambda(n) = \begin{cases} \log p, & \text{if } n = p^k, p \in \mathcal{P}, k \in \mathbb{N} \\ 0, & \text{else} \end{cases}.$$

Λ is known as the "von Mangoldt function", and will ultimately be the function of concern. We see that

$$g^*(N) = \sum_{p_1+p_2+p_3=N} \log(p_1)\log(p_2)\log(p_3) \le r(N)\log^3 N,$$

so it would suffice for us to show that there exist $C > 0$ and $N_0 \in \mathbb{N}$ such that $g^*(N) \ge CN^2$ for all $N \ge N_0$. The following lemma shows that we can actually replace g with Λ.

Lemma 1. *There exists a constant C such that $|\Lambda^*(N) - g^*(N)| \le CN^{\frac{3}{2}} \log N$ for all $N \in \mathbb{N}$.*

Proof.

$$\begin{aligned} |\Lambda^*(N) - g^*(N)|/6 &\le \sum_{\substack{p_1^{k_1}+p_2^{k_2}+p_3^{k_3}=N \\ k_1 \ge 2}} \log p_1 \log p_2 \log p_3 \\ &\le \log N \sum_{p_1\sqrt{N}, p_2 \le N} (\log_{p_1} N \log_{p_2} N)(\log p_1 \log p_2) \\ &= \sum_{p_1\sqrt{N}, p_2 \le N} \log^3 N \le CN^{\frac{3}{2}} \log N \text{ by the prime number theorem.} \end{aligned}$$

□

Our attention will now be focused on the von Mangoldt function, and since we're done comparing these convolutions, we will use the notation $\mathcal{R}(N) = \Lambda^*(N)$. The full result is encapsulated in the following asympotic formula for $\mathcal{R}(N)$, the derivation of which will be our ultimate goal.

Theorem 2 (Vinogradov, Quantitative Restatement)**.** *For any fixed $A > 0$,*

$$\mathcal{R}(N) = \frac{\mathfrak{S}(N)}{2}N^2 + O(\frac{N^2}{\log^A N}),$$

where

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

We see that $\mathfrak{S}(N) = 0$ for N even, but if we could show that $\mathfrak{S}(N)$ is bounded uniformly above and below by positive constants for all odd N, then this formula would indeed yield a stronger result than previously stated. This turns out to be pretty easy.

Lemma 2.

$$\frac{1}{2} < \frac{1}{\zeta(2)} \leq \mathfrak{S}(N) \leq \frac{2}{2 - \zeta(3)} < 3 \text{ for all } N \text{ odd.}$$

Proof. The outermost inequalities were inserted for aesthetic purposes only, and follow from the fact that $\zeta(2) = \frac{\pi^2}{6} < 2$, and $\zeta(3) \approx 1.2$, so we turn our attention to the middle.

For N odd,

$$\frac{1}{\mathfrak{S}(N)} \leq \prod_{p\geq 3}(\frac{1}{1 - \frac{1}{(p-1)^2}}) \leq \prod_{\mathcal{P}}(\frac{1}{1 - \frac{1}{p^2}}) = \zeta(2),$$

and for all N,

$$\frac{1}{\mathfrak{S}(N)} \geq \prod_{\mathcal{P}}(\frac{1}{1 + \frac{1}{(p-1)^3}}) = \frac{1}{2}\cdot\prod_{p\geq 3}(\frac{1}{1 + \frac{1}{(p-1)^3}}) \geq \frac{1}{2}\cdot\prod_{\mathcal{P}}\frac{1}{1 + \frac{1}{p^3}}$$

$$= \frac{1}{2}\sum_{k=1}^{\infty}\frac{(-1)^{\sum_{\mathcal{P}} \mathrm{ord}_p(k)}}{k^3} \geq \frac{1}{2}(1 - \sum_{k=2}^{\infty}\frac{1}{k^3}) = \frac{2 - \zeta(3)}{2}.$$

□

Now our goal is more clear and we proceed with deriving the asymptotic formula via the Hardy-Littlewood Circle Method. For this, we must partition the circle into major and minor arcs, much like in Waring, where we thought of the major arcs as those points which were "close to rationals with small denominator." However, what we took as our meanings of "close" and "small denominator" were inspired by the Weyl Inequality and the range of denominators for which it provided a worthwhile estimate. The same will be the case here, but we need an analog to the Weyl Inequality in terms of the von Mangoldt function, and we will define the major and minor arcs appropriately based on that estimate.

Lemma 3. *If $\alpha \in [0, 1]$ and $|\alpha - a/q| < 1/q^2$ for some $q \in \mathbb{N}$ and $(a, q) = 1$, then*

$$|\widehat{\Lambda}_N(\alpha)| \leq C(Nq^{-\frac{1}{2}} + N^{\frac{4}{5}} + N^{\frac{1}{2}}q^{\frac{1}{2}})\log^4 N$$

for some absolute constant C.

Lemma 3 was Vinogradov's main achievement in proving this theorem unconditionally. Hardy and Littlewood attained the result in the 1920's, but they needed to assume the Generalized Riemann Hypothesis to get the required estimate on the minor arcs.

Corollary 4. *If we suppose further that, for a fixed $B > 0$, $\log^B N \leq q \leq \frac{N}{\log^B N}$, then*

$$|\widehat{\Lambda}_N(\alpha)| \leq C\Big(\frac{N}{\log^{\frac{B}{2}} N} + N^{\frac{4}{5}} + \frac{N}{\log^{\frac{B}{2}} N}\Big)\log^4 N \leq C'\frac{N}{\log^{\frac{B}{2}-4} N}.$$

Now, given a fixed $A > 0$ as in Theorem 2, we set $B = 2A + 10$ and we define the major and minor arcs as follows.

Definition. For $(a, q) = 1$, we define the arc

$$\mathbf{M}_{\frac{a}{q}} = \{\alpha \in [0,1] \mid |\alpha - \frac{a}{q}| < \frac{\log^B N}{N}\},$$

the *major arcs*

$$\mathfrak{M} = \bigcup_{q=1}^{\log^B N} \bigcup_{\substack{0\leq a\leq q\\(a,q)=1}} \mathbf{M}_{\frac{a}{q}},$$

and the *minor arcs*

$$\mathfrak{m} = [0,1] \setminus \mathfrak{M}.$$

Lemma 5. *For sufficiently large N, $\mathfrak{M}$ comprises a small portion of the circle and the individual arcs in $\mathfrak{M}$ are pairwise disjoint.*

Proof. The first part is clear from the definition, as the measure of $\mathfrak{M}$ is at most $\frac{2\log^{3B} N}{N}$. The second part requires only slightly more argument, so let's assume $\alpha \in \mathbf{M}_{\frac{a}{q}} \bigcap \mathbf{M}_{\frac{a'}{q'}}$ with $\frac{a}{q} \neq \frac{a'}{q'}$, then we have

$$\frac{1}{qq'} \leq |\frac{a}{q} - \frac{a'}{q'}| \leq |\alpha - \frac{a}{q}| + |\alpha - \frac{a'}{q'}| \leq \frac{2\log^B N}{N}$$

which implies

$$\max\{q, q'\} \geq \Big(\frac{N}{2\log^B N}\Big)^{1/2} > \log^B N$$

for sufficiently large N, i.e. one of the original arcs was not in the collection of major arcs, since its corresponding denominator was too large. □

The following estimate on the minor arcs follows almost immediately from the definition and Lemma 3.

Lemma 6. *There exists a constant C such that*

$$|\widehat{\Lambda}_N(\alpha)| \leq C\frac{N}{\log^{\frac{B}{2}-4} N}$$

for all $\alpha \in \mathfrak{m}$.

Proof. Fix $\alpha \in \mathfrak{m}$. By the Dirichlet Principle, there exists $1 \leq q \leq \frac{N}{\log^B N}$ and $(a, q) = 1$ with

$$|\alpha - \frac{a}{q}| < \frac{\log^B N}{qN} \leq \frac{1}{q^2}.$$

But, since $\alpha \in \mathfrak{m}$ and $|\alpha - \frac{a}{q}| < \frac{\log^B N}{N}$, we must have $q > \log^B N$.

Therefore, q lies in the required range for Corollary 4 and the estimate applies. □

Corollary 7.
$$|\int_{\mathfrak{m}} (\widehat{\Lambda}_N(\alpha))^3 e^{2\pi i N\alpha} d\alpha| \le C\frac{N^2}{\log^A N}.$$

Proof. Recall Plancherel's Identity, which states in particular that
$$\int_0^1 |\widehat{\Lambda}_N(\alpha)|^2 d\alpha = \sum_{k=1}^{N} |\Lambda(k)|^2.$$
From this fact, Lemma 6, and the prime number theorem, we have
$$\begin{aligned}
|\int_{\mathfrak{m}} (\widehat{\Lambda}_N(\alpha))^3 e^{2\pi i N\alpha} d\alpha| &\le \int_{\mathfrak{m}} |\widehat{\Lambda}_N(\alpha)|^3 d\alpha \le C\frac{N}{\log^{\frac{B}{2}-4} N}\int_0^1 |\widehat{\Lambda}_N(\alpha)|^2 d\alpha \\
&= C\frac{N}{\log^{\frac{B}{2}-4} N}\sum_{k=1}^{N} |\Lambda(k)|^2 \le C'\frac{N}{\log^{\frac{B}{2}-4} N}\cdot N\log N \\
&= C'\frac{N^2}{\log^{\frac{B}{2}-5} N} = C'\frac{N^2}{\log^A N}.
\end{aligned}$$
□

This tells us that the contribution from the minor arcs to the integral $\mathcal{R}(N)$ can be absorbed into the error term from the asymptotic formula, so if we take Lemma 3 on faith, then we can turn our attention to the major arcs. In order to estimate the integral over the major arcs, we need to estimate $\widehat{\Lambda}_N$ near rationals with small denominator, so it's only natural to begin by considering $\widehat{\Lambda}_N$ **at** rationals with small denominator.

Definition. For $N, r, q \in \mathbb{N}$, we define
$$\psi_N(r,q) = \sum_{\substack{1\le k\le N \\ k\equiv r (\text{mod q})}} \Lambda(k),$$
and note that
$$\begin{aligned}
\widehat{\Lambda}_N(\frac{a}{q}) &= \sum_{k=1}^{N} \Lambda(k)e^{-2\pi i k\frac{a}{q}} = \sum_{r=o}^{q-1} \sum_{\substack{1\le k\le N \\ k\equiv r (\text{mod q})}} \Lambda(k)e^{-2\pi i k\frac{a}{q}} \\
&= \sum_{r=o}^{q-1} \sum_{\substack{1\le k\le N \\ k\equiv r (\text{mod q})}} \Lambda(k)e^{-2\pi i r\frac{a}{q}} = \sum_{r=0}^{q-1} \psi_N(r,q)e^{-2\pi i r\frac{a}{q}}.
\end{aligned}$$

To estimate this rephrased sum, we invoke a useful identity, which we will prove, and a famous theorem, which we will not.

Lemma 8 (Siegel-Walfisz Theorem, 1936)**.** *If $(r,q) = 1$ and $1 \le q \le \log^B N$, then there exists a constant $c_B > 0$ such that*
$$\psi_N(r,q) = \frac{N}{\phi(q)} + O(Ne^{-c_B\sqrt{\log N}}).$$

This is a quantitative strengthening of Dirichlet's Theorem on primes in arithmetic progressions. Roughly, it states that the primes are "evenly distributed" in the congruence classes coprime to q.

Lemma 9 (Ramanujan Sum)**.** *If $(a,q)=1$, then*

$$\sum_{\substack{0\le r\le q-1\\(r,q)=1}} e^{-2\pi i ra/q} = \mu(q),$$

where $\mu(q)$ is the standard Möbius function.

Proof. Recall that

$$\sum_{d|n}\mu(d) = \begin{cases}1 & n=1\\ 0 & \text{else}\end{cases},$$

so we can write

$$\sum_{\substack{0\le r\le q-1\\(r,q)=1}} e^{-2\pi i ra/q} = \sum_{r=0}^{q-1}\sum_{d|(r,q)}\mu(d)e^{-2\pi ra/q},$$

which, after switching the order of summation, equals

$$\begin{aligned}\sum_{d|q}\mu(d)\sum_{\substack{0\le r\le q-1\\ d|r}} e^{-2\pi i ra/q} &= \sum_{d|q}\mu(d)\sum_{l=0}^{\frac{q}{d}-1} e^{-2\pi i lda/q}\ \text{(setting } r=ld)\\ &= \sum_{d|q}\mu(d)\cdot\begin{cases}\frac{q}{d} & \text{if } d=q\\ 0 & \text{else}\end{cases} = \mu(q).\end{aligned}$$

□

Lemmas 8 and 9, plus a little additional elbow grease, yield the following estimate.

Lemma 10. *If $(a,q)=1$ and $1\le q\le \log^B N$, then there exists $c_B>0$ such that*

$$\widehat{\Lambda}_N\left(\frac{a}{q}\right) = \frac{\mu(q)}{\phi(q)}N + O(Ne^{-c_B\sqrt{\log N}}).$$

Proof. We first note that the primary contributions to the rewritten sum $\widehat{\Lambda}_N(\frac{a}{q})$ come from classes r which are coprime to q. More specifically,

$$\begin{aligned}|\sum_{\substack{0\le r\le q-1\\(r,q)>1}}\psi_N(r,q)e^{-2\pi i ra/q}| &\le \sum_{\substack{0\le r\le q-1\\(r,q)>1}}\ \sum_{\substack{1\le k\le N\\ k\equiv r(\text{mod q})}}\Lambda(k) \le \sum_{\substack{p|q\\ p^k\le N}}\log p\\ &\le \sum_{p|q}(\log_p N)(\log p) = \log N\cdot\#\{p|q\} \le C\log^2 N.\end{aligned}$$

Now we proceed by substituting in the results from the lemmas.

$$\widehat{\Lambda}_N\Big(\frac{a}{q}\Big) = \sum_{r=0}^{q-1} \psi_N(r,q) e^{-2\pi i r \frac{a}{q}} = \sum_{\substack{0\le r\le q-1\\(r,q)=1}} \psi_N(r,q) e^{-2\pi i r \frac{a}{q}} + \sum_{\substack{0\le r\le q-1\\(r,q)>1}} \psi_N(r,q) e^{-2\pi i r \frac{a}{q}}$$

$$= \sum_{\substack{0\le r\le q-1\\(r,q)=1}} \Big(\frac{N}{\phi(q)} + O(Ne^{-c_B\sqrt{\log N}})\Big) e^{-2\pi i r \frac{a}{q}} + O(\log^2 N)$$

$$= \frac{N}{\phi(q)} \sum_{\substack{0\le r\le q-1\\(r,q)=1}} e^{-2\pi i r \frac{a}{q}} + O(qNe^{-c_B\sqrt{\log N}}) + O(\log^2 N)$$

$$= \frac{\mu(q)}{\phi(q)} N + O(Ne^{-c'_B\sqrt{\log N}}).$$

□

In order to extend our estimate to all of the major arcs, we utilize the summation by parts formula

$$\sum_{k=1}^{N} a_k b_k = S_N b_{N+1} + \sum_{k=1}^{N} S_k (b_k - b_{k+1}), \text{ where } S_k = a_1 + a_2 + \cdots + a_k,$$

including the special case

$$\sum_{k=1}^{N} b_k = N b_{N+1} + \sum_{k=1}^{N} k(b_k - b_{k+1}).$$

With these facts and Lemma 10, we get the following estimates for $\widehat{\Lambda}_N$ on $\mathfrak{M}$.

Lemma 11. *If $\alpha = \frac{a}{q} + \beta$, $(a,q)=1$, $1 \le q \le \log^B N$, and $|\beta| < \frac{\log^B N}{N}$, then there exists $c_B > 0$ such that*

$$\widehat{\Lambda}_N(\alpha) = \frac{\mu(q)}{\phi(q)} \nu_N(\beta) + O(Ne^{-c_B\sqrt{\log N}}),$$

where

$$\nu_N(\beta) = \sum_{k=1}^{N} e^{-2\pi i N\beta}.$$

Proof.

$$\widehat{\Lambda}_N(\alpha) = \sum_{k=1}^{N} \Lambda(k) e^{-2\pi i k \frac{a}{q}} e^{-2\pi i k\beta},$$

so setting $a_k = \Lambda(k) e^{-2\pi i k \frac{a}{q}}$ and $b_k = e^{-2\pi i k\beta}$ in the summation by parts formula, Lemma 10 yields

$$\begin{aligned}
\widehat{\Lambda}_N(\alpha) &= \widehat{\Lambda}_N(\frac{a}{q})e^{-2\pi i(N+1)\beta} + \sum_{k=1}^{N}\widehat{\Lambda}_k(\frac{a}{q})(e^{-2\pi ik\beta} - e^{-2\pi i(k+1)\beta}) \\
&= (\frac{\mu(q)}{\phi(q)}N + O(Ne^{-c_B\sqrt{\log N}}))e^{-2\pi i(N+1)\beta} + \sum_{k=1}^{N}(\frac{\mu(q)}{\phi(q)}k + O(Ne^{-c_B\sqrt{\log N}}))(e^{-2\pi ik\beta} - e^{-2\pi i(k+1)\beta}) \\
&= \frac{\mu(q)}{\phi(q)}(Ne^{-2\pi i(N+1)\beta} + \sum_{k=1}^{N}k(e^{-2\pi ik\beta} - e^{-2\pi i(k+1)\beta})) \\
&+ O(Ne^{-c_B\sqrt{\log N}}) + \sum_{k=1}^{N}O(Ne^{-c_B\sqrt{\log N}})e^{-2\pi ik\beta}(1 - e^{2\pi i\beta}),
\end{aligned}$$

which, by the aforementioned special case of summation by parts and the fact that $|1-e^{2\pi i\beta}| < C|\beta|$ and $|\beta| < \frac{\log^B N}{N}$, equals

$$\begin{aligned}
\frac{\mu(q)}{\phi(q)}\sum_{k=1}^{N}e^{-2\pi ik\beta} + O((1+|\beta|N)Ne^{-c_B\sqrt{\log N}}) &= \frac{\mu(q)}{\phi(q)}\nu_N(\beta) + O((\log^B N)Ne^{-c_B\sqrt{\log N}} \\
&= \frac{\mu(q)}{\phi(q)}\nu_N(\beta) + O(Ne^{-c'_B\sqrt{\log N}}).
\end{aligned}$$

□

Corollary 12.

$$\int_{\mathfrak{M}}(\widehat{\Lambda}_N(\alpha))^3 e^{2\pi iN\alpha}d\alpha = \sum_{q=1}^{\log^B N}\frac{\mu(q)}{\phi(q)^3}C_q(N)\int_{|\beta|<\frac{\log^B N}{N}}(\nu_N(\beta))^3 e^{2\pi iN\beta}d\beta + O(N^2 e^{-c_B\sqrt{\log N}}),$$

where

$$C_q(N) = \sum_{\substack{0\le a\le q-1\\(a,q)=1}} e^{2\pi iNa/q}.$$

Proof. For sufficiently large N, by Lemma 5,

$$\begin{aligned}
\int_{\mathfrak{M}}(\widehat{\Lambda}_N(\alpha))^3 e^{2\pi iN\alpha}d\alpha &= \sum_{q=1}^{\log^B N}\sum_{\substack{0\le a\le q-1\\(a,q)=1}}\int_{\mathbf{M}_{\frac{a}{q}}}(\widehat{\Lambda}_N(\alpha))^3 e^{2\pi iN\alpha}d\alpha \\
&= \sum_{q=1}^{\log^B N}\sum_{\substack{0\le a\le q-1\\(a,q)=1}}\int_{|\beta|<\frac{\log^B N}{N}}(\frac{\mu(q)}{\phi(q)}\nu_N(\beta) + O(Ne^{-c_B\sqrt{\log N}}))^3 e^{2\pi iN(a/q+\beta)}d\beta,
\end{aligned}$$

which, after applying the binomial theorem to the error term and noting that $\mu(q)^3 = \mu(q)$, equals

$$\sum_{q=1}^{\log^B N}\sum_{\substack{0\le a\le q-1\\(a,q)=1}}\int_{|\beta|<\frac{\log^B N}{N}}(\frac{\mu(q)}{\phi(q)^3}(\nu_N(\beta))^3 + O(N^3 e^{-c_B\sqrt{\log N}}))e^{2\pi iN(a/q+\beta)}d\beta$$

$$= \sum_{q=1}^{\log^B N} \frac{\mu(q)}{\phi(q)^3} \sum_{\substack{0\le a\le q-1\\(a,q)=1}} e^{2\pi i N \frac{a}{q}} \int_{|\beta|<\frac{\log^B N}{N}} ((\nu_N(\beta))^3 + O(N^3 e^{-c_B\sqrt{\log N}}))e^{2\pi i N\beta} d\beta$$

$$= \sum_{q=1}^{\log^B N} \frac{\mu(q)}{\phi(q)^3} C_q(N) \int_{|\beta|<\frac{\log^B N}{N}} (\nu_N(\beta))^3 e^{2\pi i N\beta} d\beta + O(N^2(\log^B N)e^{-c_B\sqrt{\log N}})$$

$$= \sum_{q=1}^{\log^B N} \frac{\mu(q)}{\phi(q)^3} C_q(N) \int_{|\beta|<\frac{\log^B N}{N}} (\nu_N(\beta))^3 e^{2\pi i N\beta} d\beta + O(N^2 e^{-c'_B\sqrt{\log N}}).$$ □

To make better sense of this estimate we use the following two lemmas, from which the asymptotic formula for $\mathcal{R}(N)$ will follow.

Lemma 13.

$$\int_{|\beta|<\frac{\log^B N}{N}} (\nu_N(\beta))^3 e^{2\pi i N\beta} d\beta = \frac{N^2}{2} + O(\frac{N^2}{\log^{2B} N}).$$

Proof. We first note that $\int_0^1 (\nu_N(\beta))^3 e^{2\pi i N\beta} d\beta$ is simply the number of ways of writing N as the sum of three natural numbers ($1^*_{\mathbb{N}}(N)$ in our previous notation). Once the first two natural numbers n_1, n_2, are chosen with $2 \le n_1 + n_2 \le N-1$, then there is exactly one choice for the third natural number, $n_3 = N - n_1 - n_2$. Of course, for each $2 \le k \le N-1$, there are exactly $k-1$ ways to write $k = n_1 + n_2$. In other words,

$$\int_0^1 (\nu_N(\beta))^3 e^{2\pi i N\beta} d\beta = \sum_{k=2}^{N-1} k - 1 = \sum_{k=1}^{N-2} k = \frac{(N-2)(N-1)}{2} = \frac{N^2}{2} + O(N).$$

Therefore, it will suffice to show

$$\int_{|\beta|<\frac{\log^B N}{N}} (\nu_N(\beta))^3 e^{2\pi i N\beta} d\beta = \int_0^1 (\nu_N(\beta))^3 e^{2\pi i N\beta} d\beta + O(\frac{N^2}{\log^{2B} N}).$$

Recall the following estimate on the geometric series, which we used in our discussion of Waring to prove the Weyl Inequality.

$$|\nu_N(\beta)| = |\sum_{k=1}^{N} e^{-2\pi i k\beta}| \le \min\{N, \frac{1}{\|\beta\|}\} \le C\frac{N}{1+N\|\beta\|}, \text{ where } \|\beta\| = \min_{n\in\mathbb{Z}} |\beta - n|.$$

Applying this estimate, we have

$$|\int_0^1 (\nu_N(\beta))^3 e^{2\pi i N\beta} d\beta - \int_{|\beta|<\frac{\log^B N}{N}} (\nu_N(\beta))^3 e^{2\pi i N\beta} d\beta| \le \int_{\frac{\log^B N}{N}}^{1-\frac{\log^B N}{N}} |\nu_N(\beta)|^3 d\beta$$

$$\le C \int_{\frac{\log^B N}{N}}^{1-\frac{\log^B N}{N}} (\frac{N}{1+N\|\beta\|})^3 d\beta = 2C \int_{\frac{\log^B N}{N}}^{\frac{1}{2}} (\frac{N}{1+N\beta})^3 d\beta = 2CN^2 \int_{\log^B N}^{\frac{N}{2}} \frac{1}{(1+\beta)^3} d\beta$$

$$= CN^2 \Big[\frac{-1}{(1+\beta)^2}\Big]_{\log^B N}^{\frac{N}{2}} \le C\frac{N^2}{\log^{2B} N},$$

and the result follows. □

Lemma 14.

$$\sum_{q=1}^{\log^B N} \frac{\mu(q)}{\phi(q)^3} C_q(N) = \mathfrak{S}(N) + O(\frac{1}{\log^{\frac{B}{2}} N}).$$

Proof. First we will show that

$$\sum_{q=1}^{\log^B N} \frac{\mu(q)}{\phi(q)^3} C_q(N) = \sum_{q=1}^{\infty} \frac{\mu(q)}{\phi(q)^3} C_q(N) + O(\frac{1}{\log^{\frac{B}{2}} N}).$$

Recall that for every $\epsilon > 0$, there exists a constant $c_\epsilon > 0$ such that $\phi(k) \geq c_\epsilon k^{1-\epsilon}$ for every $k \in \mathbb{N}$, so in particular, we can fix $c = c_{\frac{3}{4}}$. We also see that $|C_q(N)| \leq \phi(q)$ for all q. Combining these facts, we have

$$|\sum_{q=1}^{\infty} \frac{\mu(q)}{\phi(q)^3} C_q(N) - \sum_{q=1}^{\log^B N} \frac{\mu(q)}{\phi(q)^3} C_q(N)| \leq \sum_{\log^B N}^{\infty} \frac{|C_q(N)|}{\phi(q)^3}$$
$$\leq C \sum_{\log^B N}^{\infty} \frac{1}{q^{\frac{3}{2}}} \leq C' \int_{\log^B N}^{\infty} \frac{1}{x^{\frac{3}{2}}} dx \leq \frac{C''}{\log^{\frac{B}{2}} N}.$$

Now it will suffice to show that $\sum_{q=1}^{\infty} \frac{\mu(q)}{\phi(q)^3} C_q(N) = \mathfrak{S}(N)$. We see that $A_N(q) = \frac{\mu(q)}{\phi(q)^3} C_q(N)$ is a multiplicative function of q, as μ and ϕ are known to be multiplicative, and $C_q(N)$ can be seen to be multiplicative in q by the Chinese Remainder Theorem. We can also see, by arguments similar to those above, that $\sum_{q=1}^{\infty} |A_N(q)| < \infty$. Therefore, we can write

$$\sum_{q=1}^{\infty} A_N(q) = \prod_{p \in \mathcal{P}} \sum_{k=0}^{\infty} A_N(p^k).$$

However, by the definition of the Möbius function μ, $A_N(p^k) = 0$ for all $p \in \mathcal{P}, k \geq 2$. This yields

$$\sum_{q=1}^{\infty} A_N(q) = \prod_{p \in \mathcal{P}} (1 + \frac{\mu(p)}{\phi(p)^3} C_p(N)).$$

We know that $\phi(p) = p - 1$ and $\mu(p) = -1$, and we can see that

$$C_p(N) = \begin{cases} p-1 & \text{if } p|N \\ -1 & \text{if } p \nmid N \end{cases}.$$

Putting it all together, we have

$$\sum_{q=1}^{\infty} A_N(q) = \prod_{p \in \mathcal{P}} (1 - \frac{C_p(N)}{(p-1)^3}) = \prod_{p|N} (1 - \frac{1}{(p-1)^2}) \prod_{p \nmid N} (1 + \frac{1}{(p-1)^3}) = \mathfrak{S}(N),$$

and the result follows. ∎

We are now ready to put the final pieces together. In particular, we will directly apply Corollary 7, Corollary 12, Lemma 13, and Lemma 14.

Proof of Theorem 2.

$$\begin{aligned}
\mathcal{R}(N) &= \int_0^1 (\widehat{\Lambda}_N(\alpha))^3 e^{2\pi i N\alpha} d\alpha = \int_{\mathfrak{M}} (\widehat{\Lambda}_N(\alpha))^3 e^{2\pi i N\alpha} d\alpha + \int_{\mathfrak{m}} (\widehat{\Lambda}_N(\alpha))^3 e^{2\pi i N\alpha} d\alpha \\
&= \sum_{q=1}^{\log^B N} \frac{\mu(q)}{\phi(q)^3} C_q(N) \int_{|\beta| < \frac{\log^B N}{N}} (\nu_N(\beta))^3 e^{2\pi i N\beta} d\beta + O(N^2 e^{-C_B\sqrt{\log N}}) + O(\frac{N^2}{\log^A N}) \\
&= (\mathfrak{S}(N) + O(\frac{1}{\log^{\frac{B}{2}} N}))(\frac{N^2}{2} + O(\frac{N^2}{\log^{2B} N})) + O(\frac{N^2}{\log^A N}) \\
&= \frac{\mathfrak{S}(N)}{2} N^2 + O(\frac{N^2}{\log^A N}).
\end{aligned}$$

□

We have now shown not only that every sufficiently large odd integer is the sum of three primes, but also that the order of growth of the number of representations of an odd integer as the sum of three primes agrees with our expectation.

2. A partial result of the binary Goldbach Conjecture

Using a similar heuristic as before, we could also guess that the number of representations of an *even* natural number N as the sum of *two* primes would be on the order of $\frac{N}{\log^2 N}$. Using the same estimates we have already obtained in our exposition of Vinogradov's Theorem, we can show that this is the case for "almost every" even integer, in an appropriate sense, yielding another a partial result to the binary Goldbach Conjecture, also originally obtained in the late 1930s.

Recall that for $S \subseteq \mathbb{N}$, the density of S, denoted $\delta(S)$, is defined as

$$\delta(S) = \lim_{N\to\infty} \frac{|S \cap [1, N]|}{N},$$

if the above limit exists. We wish to investigate the density of a particular set of integers, the "bad guys" if you will.

Definition. Let $E = \{n \in \mathbb{N} \text{ even } | n \notin \mathcal{P} + \mathcal{P}\}$, and $E_N = E \cap [1, N]$.

Note that Goldbach's Conjecture is precisely the statement that $E = \{2\}$. We will obtain the weaker result that $\delta(E) = 0$, or equivalently $\delta(\mathcal{P} + \mathcal{P}) = 1/2$, the statement that almost every even integer is the sum of two primes. We start by defining the appropriate weighted count and the corresponding singular series, analogous to what we did previously.

Definition. We define

$$G(N) = \sum_{k_1+k_2=N} \Lambda(k_1)\Lambda(k_2) = \int_0^1 (\widehat{\Lambda}_N(\alpha))^2 e^{2\pi i N\alpha} d\alpha,$$

$$\text{and } \mathfrak{S}_2(N) = \sum_{q=1}^{\infty} \frac{\mu(q)^2}{\phi(q)^2} C_q(N) = (\prod_{p|N} 1 + \frac{1}{p-1})(\prod_{p\nmid N} 1 - \frac{1}{(p-1)^2}).$$

The equality of the two expressions for the singular series follows in identical fashion to the corresponding formula in the ternary problem. Note that $\mathfrak{S}_2(N) = 0$ for N odd, and $\mathfrak{S}_2(N) > 1$ for N even. A direct analogy to the Vinogradov result would be an asymptotic formula of the shape

$$G(N) = \mathfrak{S}_2(N) \cdot N + O(\frac{N}{\log^A N}).$$

Such a result would be a quantitative version of Goldbach's Conjecture, and would in particular imply that E is finite. Obviously this is out of reach, but a weaker way of displaying that $G(N)$ looks like $\mathfrak{S}_2(N) \cdot N$ is to bound the mean-square difference. This turns out to be tractable, and yields the promised result.

Theorem 3. *For a fixed $A > 0$, there exists a constant C depending only on A such that*

$$\sum_{n=1}^{N} (G(n) - \mathfrak{S}_2(n) \cdot n)^2 \leq C \frac{N^3}{\log^A N}.$$

Before we get our hands dirty with this proof, let's see why it gets us what we want.

Corollary 15. $|E_N| \leq C \frac{N}{\log^A N}$, *and in particular $\delta(E) = 0$.*

Proof. If $n \in E$, then

$$\begin{aligned} G(n) = \sum_{\substack{p_1^{k_1} + p_2^{k_2} = n \\ k_1 \text{ or } k_2 \geq 2}} (\log p_1)(\log p_2) &\leq \sum_{\substack{p^k \leq n \\ k \geq 2}} (\log p)(\log n) \\ &\leq \sum_{p \leq \sqrt{n}} (\log_p n)(\log p)(\log n) = \sum_{p \leq \sqrt{n}} \log^2 n \leq C\sqrt{n} \log n. \end{aligned}$$

In particular, there exists $N_0 \in \mathbb{N}$ such that

$$(G(n) - \mathfrak{S}_2(n) \cdot n)^2 > \frac{n^2}{4},$$

whenever $n > N_0$ and $n \in E$. In other words, for sufficiently large n,

$$\frac{4}{n^2}(G(n) - \mathfrak{S}_2(n) \cdot n)^2 > 1_E(n),$$

which implies

$$|E_N| \leq N_0 + 4 \sum_{N_0 < n < N} \frac{1}{n^2}(G(n) - \mathfrak{S}_2(n) \cdot n)^2 \text{ for all } N > N_0.$$

Therefore, it will suffice for us to show that

$$\sum_{n=1}^{N} \frac{1}{n^2}(G(n) - \mathfrak{S}_2(n) \cdot n)^2 \leq C \frac{N}{\log^A N},$$

for which we use summation by parts. Letting $a_n = (G(n) - \mathfrak{S}_2(n) \cdot n)^2$ and $S_n = \sum_{k=1}^{n} a_k$, we have from Theorem 3 that $S_n \leq C \frac{n^3}{\log^A n}$ for all $n > 1$, so summation by parts yields

$$\sum_{n=1}^{N} \frac{a_n}{n^2} = \frac{S_N}{N^2} + \sum_{n=1}^{N} S_n (\frac{1}{n^2} - \frac{1}{(n+1)^2}) \leq C(\frac{N}{\log^A N} + \int_2^N \frac{1}{\log^A x} dx),$$

so it will suffice to show that $\displaystyle\int_2^N \frac{1}{\log^A x} dx \leq C \frac{N}{\log^A N}$.

By dividing the interval $[2, N]$, we see

$$\int_2^N \frac{1}{\log^A x} dx = \int_2^{\sqrt{N}} \frac{1}{\log^A x} dx + \int_{\sqrt{N}}^N \frac{1}{\log^A x} dx$$

$$\leq \frac{\sqrt{N}}{\log^A 2} + 2^A \frac{N}{\log^A N} \leq C \frac{N}{\log^A N}.$$

This proves the corollary, but the theorem remains. □

Proof of Theorem 3. Fix $A > 0$, and define B, $\mathfrak{M}$, and $\mathfrak{m}$ as before.

We see that $G(n) = G_1(n) + G_2(n)$, where

$$G_1(n) = \int_{\mathfrak{M}} (\widehat{\Lambda}_n(\alpha))^2 e^{2\pi i n\alpha} d\alpha$$

and

$$G_2(n) = \int_{\mathfrak{m}} (\widehat{\Lambda}_n(\alpha))^2 e^{2\pi i n\alpha} d\alpha.$$

By Cauchy-Schwarz,

$$\sum_{n=1}^N (G(n) - \mathfrak{S}_2(n) \cdot n)^2 \leq 2\Big(\sum_{n=1}^N |G_1(n) - \mathfrak{S}_2(n) \cdot n|^2 + \sum_{n=1}^N |G_2(n)|^2\Big),$$

and it will suffice to show that

$$\sum_{n=1}^N |G_1(n) - \mathfrak{S}_2(n) \cdot n|^2 \leq C \frac{N^3}{\log^A N}$$

and

$$\sum_{n=1}^N |G_2(n)|^2 \leq C \frac{N^3}{\log^A N}.$$

For the latter, we notice that $G_2(n)$ is a Fourier coefficient for $\widehat{\Lambda}_N(\alpha)^2 \cdot 1_{\mathfrak{m}}$, and hence by Bessel's inequality,

$$\sum_{n=1}^N |G_2(n)|^2 \leq \int_{\mathfrak{m}} |\widehat{\Lambda}_N(\alpha)|^4 d\alpha.$$

Invoking Lemma 6 and Plancherel's Identity, we have that

$$\sum_{n=1}^N |G_2(n)|^2 \leq C \frac{N^2}{\log^{B-8} N} \int_0^1 |\widehat{\Lambda}_N(\alpha)|^2 d\alpha = C \frac{N^2}{\log^{B-8} N} \sum_{n=1}^N |\Lambda(n)|^2$$

$$\leq C \frac{N^3}{\log^{B-9} N} \leq C \frac{N^3}{\log^A N}.$$

This need to jump to the mean-square value in order to estimate the minor arcs is the primary obstruction to obtaining a true asymptotic formula the way we did in the ternary problem.

To estimate $G_1(n)$, we invoke Lemma 11, apply arguments virtually identical to those in Corollary 12 and Lemma 13 (just replacing the cubes with squares), and after noticing that

$$\int_0^1 \nu_n(\beta)^2 e^{2\pi i n\beta} = \#\{(n_1, n_2) \in \mathbb{N}^2 | n_1 + n_2 = n\} = n - 1,$$

we obtain the following estimate for $n \le N$.

$$G_1(n) = \mathfrak{S}_2'(n) \cdot n + O(\frac{N}{\log^{\frac{B}{2}} N}), \text{ where } \mathfrak{S}_2'(n) = \sum_{q=1}^{\log^B N} \frac{\mu(q)^2}{\phi(q)^2} C_q(n).$$

Now we see that because

$$\begin{aligned}\sum_{n=1}^{N} |G_1(n) - \mathfrak{S}_2(n) \cdot n|^2 &\le 2(\sum_{n=1}^{N} |G_1(n) - \mathfrak{S}_2'(n) \cdot n|^2 + \sum_{n=1}^{N} n^2 |\mathfrak{S}_2'(n) - \mathfrak{S}_2(n)|^2) \\ &\le C(\frac{N^3}{\log^A N} + N^2 \sum_{n=1}^{N} |\mathfrak{S}_2'(n) - \mathfrak{S}_2(n)|^2),\end{aligned}$$

it will suffice to show that $\sum_{n=1}^{N} |\mathfrak{S}_2'(n) - \mathfrak{S}_2(n)|^2 \le C \frac{N}{\log^A N}$.

For this, we use the following facts:

(i) $C_q(n) = \dfrac{\mu(\frac{q}{(q,n)})\phi(q)}{\phi(\frac{q}{(q,n)})}$, a generalized version of Lemma 9

(ii) $\sum_{d=1}^{n} \dfrac{1}{\phi(d)} \le C \log n$

(iii) $\sum_{q=X}^{\infty} \dfrac{1}{\phi(q)^2} \le \dfrac{C}{X}$

From these, we obtain

$$\begin{aligned}\mathfrak{S}_2(n) - \mathfrak{S}_2'(n) &= \sum_{q=\log^B N}^{\infty} \frac{\mu(q)^2}{\phi(q)^2} \cdot \frac{\mu(\frac{q}{(q,n)})\phi(q)}{\phi(\frac{q}{(q,n)})} = \sum_{d|n} \sum_{\substack{\log^B N < q < \infty \\ (q,n)=d}} \frac{\mu(q)^2}{\phi(q)^2} \cdot \frac{\mu(\frac{q}{d})\phi(q)}{\phi(\frac{q}{d})} \\ &= \sum_{d|n} \sum_{\substack{\frac{\log^B N}{d} < q < \infty \\ (q,n)=1}} \frac{\mu(dq)^2}{\phi(dq)^2} \cdot \frac{\mu(q)\phi(dq)}{\phi(q)} \text{ (setting } q = \frac{q}{d}) \\ &= \sum_{d|n} \sum_{\substack{\frac{\log^B N}{d} < q < \infty \\ (q,n)=1}} \frac{\mu(d)^2 \mu(q)^3 \phi(d)\phi(q)}{\phi(d)^2 \phi(q)^3} \text{ (since } d|n, (q,n) = 1 \implies (d,n) = 1) \\ &= \sum_{d|n} \frac{\mu(d)^2}{\phi(d)} \sum_{\substack{\frac{\log^B N}{d} < q < \infty \\ (q,n)=1}} \frac{\mu(q)}{\phi(q)^2} \le C \sum_{d|n} \frac{\mu(d)^2}{\phi(d)} \cdot \min(\frac{d}{\log^B N}, 1),\end{aligned}$$

which yields $\mathfrak{S}_2(n) - \mathfrak{S}_2'(n) \le C \log n$, and hence

$$\begin{aligned}\sum_{n=1}^{N} |\mathfrak{S}_2'(n) - \mathfrak{S}_2(n)|^2 &\le C \log N \sum_{n=1}^{N} |\mathfrak{S}_2'(n) - \mathfrak{S}_2(n)| \\ &\le C \log N \sum_{n=2}^{N} \sum_{d|n} \frac{\mu(d)^2}{\phi(d)} \cdot \frac{d}{\log^B N} \le C \log N \sum_{d=2}^{N} \frac{N}{d} \frac{\mu(d)^2}{\phi(d)} \cdot \frac{d}{\log^B N} \\ &\le C \frac{N}{\log^{B-1} N} \sum_{d=2}^{N} \frac{1}{\phi(d)} \le C \frac{N}{\log^{B-2} N} \le C \frac{N}{\log^A N},\end{aligned}$$

and the result follows. □

References

[1] H. Davenport, *Multiplicative Number Theory*, Springer GTM 74, Third Edition, 2000.

[2] R. C. Vaughan, *The Hardy-Littlewood method*, Cambridge University Press, Second Edition, 1997.