VINOGRADOV’S THREE PRIMES THEOREM

ADAM LOTT

1. Introduction

We begin with a pair of conjectures that need no introduction.

Conjecture 1 (Weak Goldbach). Every odd number \( \geq 7 \) can be written as the sum of three prime numbers.

Conjecture 2 (Strong Goldbach). Every even number \( \geq 4 \) can be written as the sum of two prime numbers.

The goal of this paper is to outline the ideas used in the proof of the following related theorem [Vin].

Theorem 3 (Vinogradov, 1937). For \( N \in \mathbb{N} \), let \( r(N) = \sum_{a+b+c=N} \Lambda(a)\Lambda(b)\Lambda(c) \), where \( \Lambda \) is the von Mangoldt function. Then for any positive integer \( A \),

\[
r(N) = \frac{1}{2} G(N)N^2 + O_A \left( N^2 \log^{-A} N \right)
\]

where

\[
G(N) = \prod_{p \mid N} \left( 1 - \frac{1}{(p-1)^2} \right) \prod_{p \mid N} \left( 1 + \frac{1}{(p-1)^3} \right).
\]

The quantity \( r(N) \) measures the weighted number of representations of \( N \) as the sum of three prime powers. The following result relates Vinogradov’s theorem back to Goldbach’s conjecture.

Corollary 4. The weak Goldbach conjecture holds for sufficiently large integers.

Proof. First note that if \( N \) is odd, then \( G(N) \geq \prod_{p \neq 2} (1 - (p-1)^{-2}) \geq 1/2 \), so by Vinogradov’s theorem,

\[
N^2 \ll r(N) = \sum_{p_1 + p_2 + p_3 = N} \log(p_1)\log(p_2)\log(p_3) + \sum_{p_1^k + p_2^k + p_3^k = N} \log(p_1)\log(p_2)\log(p_3)
\]

\[
\ll P_3(N) \log^3 N + \text{(error)} \quad \text{where} \quad P_3(N) := \# \{(p_1, p_2, p_3) : p_1 + p_2 + p_3 = N\},
\]

implying that \( P_3(N) \gg N^2 \log^{-3} N + \text{(error)} \), which is positive for \( N \) sufficiently large. \( \square \)

Remark. If \( N \) is even, \( G(N) = 0 \), so Vinogradov’s theorem does not tell us anything. Indeed, if every sufficiently large even number \( N \) were expressible as the sum of three primes, then one of the primes must be 2, so \( N - 2 \) would be expressible as the sum of two primes, and the strong Goldbach conjecture would follow for sufficiently large integers.

2. Proof sketch

Let \( N \) be a fixed, large odd number. Define \( S(\alpha) := \sum_{n \leq N} \Lambda(n)e(\alpha n) \). The usefulness of this function comes from the relation

\[
S(\alpha)^3 = \sum_{n_1, n_2, n_3 \leq N} \Lambda(n_1)\Lambda(n_2)\Lambda(n_3)e(\alpha(n_1 + n_2 + n_3)) = \sum_{n \leq 3N} e(\alpha n) \sum_{a+b+c=n} \Lambda(a)\Lambda(b)\Lambda(c),
\]

from which we deduce

\[
\int_{0}^{1} S(\alpha)^3e(-\alpha N) d\alpha = \sum_{n \leq 3N} \sum_{a+b+c=n} \Lambda(a)\Lambda(b)\Lambda(c) \int_{0}^{1} e(\alpha(n - N)) d\alpha = r(N).
\]

Thus we have reduced the problem of counting \( r(N) \) to the problem of estimating the integral \( \int_{0}^{1} S(\alpha)^3e(-\alpha N) d\alpha \).

The technique of translating a counting problem into a problem about integrals of exponential sums is known as the Hardy-Littlewood circle method.

As motivation, let \( a/q \in [0, 1] \) be a rational number in lowest terms and let’s examine \( S(a/q) \).

Fact 5. If \( (k, q) = 1 \), then \( \phi(q)e(k/q) = \sum_{\chi(q)} \chi(k)\tau(\overline{\chi}) \) where \( \tau(\chi) \) is the Gauss sum \( \sum_{m/q} \chi(m)e(m/q) \).

Date: December 2, 2018.
Using this with \( k = an \), we calculate
\[
S(a/q) \approx \sum_{n \leq N} \Lambda(n)e(an/q) = \frac{1}{\phi(q)} \sum_{n \leq N} \Lambda(n) \frac{1}{\phi(q)} \sum_{\chi} \chi(an)\tau(\chi) = \frac{1}{\phi(q)} \sum_{\chi} \tau(\chi)\chi(a) \sum_{n \leq N} \chi(n)\Lambda(n)
\]
where here and throughout, the symbol \( \approx \) denotes the presence of an error term which can be shown to be negligible. Now we appeal to the heavy machinery developed in class and some other elementary facts.

**Fact 6** (Siegel-Walfisz theorem). If \( A \) is any positive integer, then uniformly for \( q \leq Q := \log^A N \), we have \( \psi(N, \chi_0) \approx N \) and \( \psi(N, \chi) \approx 0 \) for \( \chi \neq \chi_0 \).

**Fact 7.** \( \tau(\chi_0) = \mu(q) \) where \( \mu \) is the Möbius function.

Applying these to the above computation, we arrive at
\[
S(a/q) \approx \frac{\mu(q)}{\phi(q)} N. \tag{1}
\]

We now break our analysis into two cases, depending on if \( \alpha \) is close to rational numbers with small denominator (the **major arcs**) or not (the **minor arcs**). Let
\[
\mathcal{M} := \bigcup_{q \leq Q} \mathcal{M}(a,q) := \bigcup_{q \leq Q} \left[ \frac{a}{q} - \frac{1}{R}, \frac{a}{q} + \frac{1}{R} \right]
\]
\[
m := [0,1] \setminus \mathcal{M}
\]
where \( Q := \log_{\text{Co}(A)} N \) and \( R \) is a parameter to be chosen. One constraint is that \( R \) be chosen large enough so that all of the \( \mathcal{M}(a,q) \) are disjoint and \( m \) has positive measure.

2.1. **Major arcs.** We estimate the contribution of \( \mathcal{M} \) to the total integral by
\[
\int_{\mathcal{M}} S(\alpha)^3e(-\alpha N) \, d\alpha = \sum_{q \leq Q, (a,q)=1} \int_{\mathcal{M}(a,q)} S(\alpha)^3e(-\alpha N) \, d\alpha \approx \frac{1}{R} N^2 \sum_{q \leq Q} \frac{\mu(q)}{\phi(q)}^3 \sum_{(a,q)=1} e(aN/q) \tag{2}
\]
\[
\leq \frac{N^3}{R} G(N), \tag{3}
\]
where we have used another elementary fact:

**Fact 8** (Ramanujan sums).
\[
\sum_{q=1}^\infty \frac{\mu(q)}{\phi(q)}^3 \sum_{(a,q)=1} e(aN/q) = G(N).
\]

When this proof is done for real, one chooses \( R \) to be around \( \asymp N \), which when applied to equation (3) yields the correct order of magnitude for the main term in Vinogradov’s theorem.\footnote{Actually, the right choice is \( R = N \log^{-C_1(A)} N \), but our approximation is very rough and without doing the full calculation it’s impossible to see how the true main term appears.}

2.2. **Minor arcs.** We now estimate the contribution of \( m \) to the integral and show that it is negligible compared to the main term. We immediately have the estimate
\[
\left| \int_{m} S(\alpha)^3e(-\alpha N) \, d\alpha \right| \leq \sup_{\alpha \in m} |S(\alpha)| \int_0^1 |S(\alpha)|^2 \, d\alpha = \sup_{\alpha \in m} |S(\alpha)| \int_0^1 \sum_{n,m \leq N} \Lambda(n)\Lambda(m)e(\alpha(n - m)) \, d\alpha \tag{4}
\]
\[
= \sup_{\alpha \in m} |S(\alpha)| \sum_{n,m \leq N} \Lambda(n)\Lambda(m) \int_0^1 e(\alpha(n - m)) \, d\alpha = \sup_{\alpha \in m} |S(\alpha)| \sum_{n \leq N} \Lambda(n)^2 \tag{5}
\]
\[
\leq N \log^2 N \cdot \sup_{\alpha \in m} |S(\alpha)|. \tag{6}
\]

Thus we only need to prove a pointwise estimate for \( S(\alpha) \) for \( \alpha \) far away from rationals with small denominator.

To do so, we recall Vaughan’s identity.
Fact 9 (Vaughan’s identity). Let \( F(s) = \sum_{m \leq U} \Lambda(m)m^{-s} \) and \( G(s) = \sum_{d \leq V} \mu(d)d^{-s} \) where \( U \) and \( V \) are any positive real numbers. Then
\[
-\frac{\zeta'(s)}{\zeta(s)} = F(s) - \zeta(s)F(s)G(s) - \zeta'(s)G(s) + \left(-\frac{\zeta'(s)}{\zeta(s)} - F(s)\right)(1 - \zeta(s)G(s)).
\]

Comparing the Dirichlet coefficients of both sides, we obtain an expression for \( \Lambda(n) \) in terms of some complicated sums. Then to estimate \( S(\alpha) \), we multiply through by \( e(na) \) and sum over \( n \leq N \). After a lot of technical and careful estimation, and further assuming that \( \alpha \) is close to a rational number (the details can be found in sections 24 and 25 of [1]), we can obtain the following estimate.

Fact 10. If \(|a - a/q| \leq 1/q^2\), then
\[
|S(\alpha)| \ll \left( \frac{N}{\sqrt{q}} + N^{4/5} + \sqrt{Nq} \right) \log^4 N.
\]

To obtain a bound suitable for Vinogradov’s theorem, we appeal to the following well-known elementary result.

Fact 11 (Dirichlet’s approximation theorem). Let \( \alpha \) be any real number. Then for any \( R \), there exists a rational number \( a/q \) in lowest terms with \( q \leq R \) and
\[
|\alpha - a/q| < \frac{1}{qR}.
\]

Let \( \alpha \in \mathbb{R} \) and let \( R = N \log^{-C_1(A)} N \) be as in the definition of the major and minor arcs. By Dirichlet’s approximation theorem, let \( q \leq R \) be such that \(|a - a/q| < 1/(qR) \leq 1/q^2\). Then we also have \(|a - a/q| < 1/R\), so by definition of the minor arcs, we must have \( q > Q = \log^{C_1(A)} N \), so by fact 10, we get
\[
|S(\alpha)| \ll \left( \frac{N}{\log^{C_1(A)} N} + N^{4/5} + (N^2 \log^{C_1(A)} N)^{1/2} \right) \log^4 N \ll \frac{N}{\log^{C_1(A)} N}. \tag{7}
\]

Substituting this into equation (6) shows that the contribution of the minor arcs is \( \ll N^2 \log^{-C_4(A)} N \), which is the claimed error term in Vinogradov’s theorem, completing the proof.

Remark. This proof of Vinogradov’s theorem relies strongly on the Siegel-Walfisz theorem. Since all of the implied constants in Siegel-Walfisz are ineffective, this proof does not yield any computable estimate for a number \( C \) such that the weak Goldbach conjecture holds for all \( N \geq C \). In 2013, Helfgott [11, 12, 13] improved this argument with more advanced estimation techniques to remove the dependence on ineffective results and prove that the weak Goldbach conjecture holds for all \( N \geq 10^{27} \). The conjecture had previously been verified computationally up to \( 10^{30} \) [3], so the weak Goldbach conjecture is in fact a theorem.

3. Comments on the strong Goldbach conjecture

What happens if we try to apply this strategy to the strong Goldbach conjecture? Define \( r_2(N) := \sum_{a+b=N} \Lambda(a)\Lambda(b) \). Analogous to the proof of corollary 4, we can show that \( P_2(N) \gg r_2(N) \log^{-2} N \) where \( P_2(N) := \#\{(p_1, p_2) : p_1 + p_2 = N\} \), and we have \( r_2(N) = \int_0^1 S(\alpha)^2 e(-\alpha N) d\alpha \). Applying analogous arguments, we can deduce the following analogous steps of the proof.

\[
S(a/q)^2 \approx \mu(q)^2 N^2/\phi(q)^2 \quad \text{(equation 1)}
\]
\[
\sum_{q=1}^{\infty} \frac{\mu(q)^2}{\phi(q)^2} \sum_{(a,q)=1} e(aN/q) = H(N) \quad \text{where } H(N) \gg 1 \text{ for } N \text{ even} \quad \text{(fact 8)}
\]
\[
\int_{1/2}^{\infty} S(\alpha)^2 e(-\alpha N) d\alpha \asymp \frac{N^2}{R} \quad \text{(equation 3)}
\]

After choosing \( R \) in the necessary way, we see that the main term is only on the order of \( N \). But now, to estimate the contribution from the minor arcs, we can use either the pointwise estimate or the square-integral estimate, but neither of these are good enough:
\[
\int_0^1 |S(\alpha)|^2 d\alpha \ll N \log^2 N \quad \text{by equation 5}
\]
\[
\sup_{\alpha \in \mathbb{C}} |S(\alpha)|^2 \ll \frac{N^2}{\log^{C_5(A)} N} \quad \text{by equation 7}.
\]

Therefore in this case, the error terms dominate the main term, so “Vinogradov’s two primes theorem” fails, so even asymptotically, the strong Goldbach conjecture remains open.
References


