Vinogradov's Theorem

Julie Griswold

April 2024

1 Introduction

In today's talk I will be discussing Vinogradov's theorem which states that every large integer is the sum of three primes. Along with this statement, Vinogradov also obtained an asymptotic formula for the number of representations of an odd integer as the sum of three primes. In this section which corresponds to section 8.1 in the textbook I will go over the counting function and asymptotic function.

Counting function for odd integers r(N):
$r(N) = \sum_{p_1+p_2+p_3=N}$

The asymptotic formula for r(N) deals with the cases of when the number of odd integers N is really large, and gives the estimate of prime numbers up to a given limit.

Theorem 8.1: There exists an arithmetic function $\mathfrak{S}(N)$ and positive constants c_1 and c_2 such that

$$c_1 < \mathfrak{S}(N) < c_2$$

for all large numbers N and

$$r(N) = \mathfrak{S}(N)\frac{N^2}{2(logN)^3}(1 + O(\frac{loglogN}{logN}))$$

where $\mathfrak{S}(N)$ is a singular series, which I will explain in the next section.

2 The singular series

In this section I will define singular series which are series involving arithmetic functions and help understand the distribution of prime numbers. In this section I will

- Define the arithmetic function $\mathfrak{S}(N)$ and $c_q(N)$
- Show that the singular series can be expressed as an infinite product over prime numbers

- Explain there are two positive constants to bound the singular series

First we have the arithmetic function:

$$\mathfrak{S}(N) = \sum_{q=1}^{\infty}(\frac{\mu(q)c_q(N)}{q^3}$$
where
$$c_q(N) = \sum_{a=1 and (q,a)=1}^{q} e(aN/q)$$

Theorem 8.2 The singular series $\mathfrak{S}(N)$converges absolutely and uniformly in N and has the Euler product

$$\mathfrak{S}(N) = \prod_p (1 + \frac{1}{(1-p)^3}) \prod_{p|N} (1 - \frac{1}{p^2 - 3p + 3})$$
There exist positive constants c_1 and c_2 such that
$$c_1 < \mathfrak{S}(N) < c_2$$
for all positive integers N. Moreover, for any $\epsilon > 0$,
$$\mathfrak{S}(N, Q) = \sum_q \frac{\mu(q)c_q(N)}{q^3} = \mathfrak{S}(N) + O(Q^{-(1-\epsilon)})$$
where the implied constant depends only on ϵ

From this Theorem we know that the arithmetic function can be expressed as an infinite product over prime numbers and this product has to be bounded by two constants. The section then goes on to prove why these two constants exist by using the circle method.

3 Decomposition into major and minor arcs

In this section we will use decomposition to understand exponential sums. The motivation of this section is to show that the major arc will correspond to the intervals where the exponential sums will have significant contributions to the integral, and the minor arcs will correspond to the where intervals of exponential sums have a small contribution. In this section I will explain:

- Define terms Q, q, and a and set up an interval for the arc and define the major and minor arc
- Use the counting function in 8.1 and write it as a weighted sum
- Use the circle method to write the weighted sum function R(N) as the integral over the major and minor arcs
- Finishing with the final result of the decomposition

First lets define terms:
Let $B > 0$

$Q = (logN)^B$ for

$1 \leq q \leq Q$

$0 \leq a \leq q$ and

$(a, q) = 1$

The major $arcM(q, a)$ is the interval consisting of all real numbers $\alpha \,\epsilon\, [0, 1]$ such that

$$|\alpha - \tfrac{a}{q}| \leq \tfrac{Q}{N}$$

Next we will use an example of an intersection to prove that the major $arcM(q, a)$ are disjoint for a large N because it does not satisfy an inequality. If you want to see the example it is in the book.

Now we will define the major arc as a set:

$$M = \cup_{q=1}^{Q} \cup_{a=0}\ and(a,q) = 1^{q} M(q, a) \subset [0, 1]$$

The set of minor arcs is:

$$m = \tfrac{[0,1]}{M}$$

Now we want to write the major and minor arc sets in the form of an integral of trigonometric polynomial over the major and minor arcs. To do so we need to use:

- a weighted sum over the representations of N as a sum of three primes $R(N) = \sum_{p_1+p_2+p_3=N} logp_1 logp_2 logp_3$
- The generating function for R(N) written as the the exponential sum over over primes $F(\alpha) = \sum_{p \leq N} (logp) e(p\alpha)$

From $R(N)$ and $F(\alpha)$ we can write

$$R(N) = \sum_{p_1+p_2+p_3=N} logp_1 logp_2 logp_3 = \int_0^1 F(\alpha)^3 e(-N\alpha) d\alpha$$

From here we can rewrite the integral as two different integrals one over the major arc and one over the minor arc.

$$= \int_M F(\alpha)^3 e(-N\alpha) d\alpha + \int_m F(\alpha)^3 e(-N\alpha) d\alpha$$

Hence we get two different integrals we wanted to represent the major and minor arc.

4 The Integral over the major arcs

In this section we are looking at the integral we found in the last section and we want to evaluate it. In order to do this we must know that the major arc portion of the integral is the product of the singular series (N) and an integral $J(N)$, and $J(N)$ we are able to evaluate. In this section I will explain:

- Give the estimate for the major arc $J(N)$ which is the integral over the major arc, and write out the simple proof
- Then using Theorem 8.3 which will help us understand the distribution of primes in arithmetic progression by giving us an estimate for the frequency of primes in arithmetic progression with respect to modulus.
- Lemma 8.2 will help us write a new function that incorporates the major and minor arcs in section 8.3 by diving it by q.
- Then we will check that $C > 2B$ for the function $F(\alpha)^3$ and $F(\alpha)$
- Then we will get the integral over the major arc and estimate it
- Finally we will be left with the estimation of the integral

Lemma 8.1 Let

$$u(\beta) = \sum_{m=1}^{N} e(m\beta)$$

then

$$J(N) = \int_{-1/2}^{1/2} u(\beta)^3 e(-N\beta)d\beta = \frac{N^2}{2} + O(N)$$

J(N) is the integral over the major arc which gives us an estimate. Then we will proof this very quickly.

Proof By Theorem 5.1, the number of representations of N as the sum of three positive integers is:

$$J(N) = \int_{-1/2}^{1/2} u(\beta)^3 e(-N\beta)d\beta$$

$$= \int_{-1/2}^{1/2} \sum_{m_1=1}^{N} \sum_{m_2=1}^{N} \sum m_3 = 1^N e((m_1 + m_2 + m_3 - N)\beta)d\beta$$

$$= \frac{N-1}{2}$$

$$= \frac{N^2}{2} + O(N)$$

Which completes the proof. The next theorem I will define will help us in the following lemma.

Theorem 8.3 Siegel-Walfisz If $q \geq 1 and (q,a) = 1$, then, for any $C > 0$

$$v(x;q,a) = \sum_{p \leq x and p \cong a (mod q)} logp = \frac{x}{\phi(q)} + O(\frac{x}{(logx)^C}$$

for all $x \geq 2, where the implied constant depends only on C$. This theorem will help us estimate $F_x(\alpha)$ in the next Lemma.

Lemma 8.2 Let

$$F_x(\alpha) = \sum_{p \leq 1} (logp)e(p\alpha)$$

Let B and C be positive real numbers. If $1 \leq q \leq Q = (logN)^B and (q,a) = 1, then$

$$F_x(a/q) = \frac{\mu(q)}{\phi(q)}x + O(\frac{QN}{(logN)^C}$$

for $1 \leq x \leq N$, where the implied constant depends only on B and C.
To proof and explain this lemma we want to consider:

- estimate $F_x(\alpha)$ when α is rational
- We use $F_x(a/q)$ because if $\alpha = a/q$ is rational
- $e(ya/q)$ is a periodic function y with period q, and $e((y+q)a/q) = e(ya/q + a) = e(ya/q)e(a) = e(ya/q) because e(x) = 1 when x is an integer.$
- $e(pa/q)$ only depends on the class of $p(mod q)$
- So we split up the sums into:

  $$F_x(\frac{a}{q}) = \sum_{r=1}^{q} \sum_{p \leq x and p \cong r(mod q)} (logp)e(\frac{pa}{q})$$

  Each of these sums can be written as $e(ra/q)$ times the sum of $log p over p \leq x which are r mod q$
- By the Siegel-Walfisz theorem we can estimate these sums.
- Then we get the sum

  $$\sum_{r=1 and (r,q)=1}^{q} e(\frac{ra}{q})(\frac{x}{\phi(q)} + O(\frac{x}{(logx)^C})) + O(logQ)$$

- We can now pull out the $\frac{x}{\phi(q)}$ and the remaining sum is by definition $c_a(q)$, which Theorem A.24 tell us is $\mu(q)$ just as long as $gcd(a,q) = 1$
- So finally we get

  $$\frac{\mu(q)}{v(q)}x + O(\frac{QN}{(logN)^C}$$

  Which is what we wanted

Lemma 8.3 Let B and C be positive real numbers with $C > 2B$. If $\alpha \epsilon M(q,a) and \beta = \alpha - a/q$, then,

$$F(\alpha) = \frac{\mu(q)}{\phi(q)}u(\beta) + O(\frac{Q^2N}{(logN)^C}$$

and

$$F(\alpha)^3 = \frac{\mu(q)}{\phi(q^3)}u(\beta)^3 + O(\frac{Q^2N^3}{(logN)^C}$$

where the implied constants depend only on B and C
To understand and proof this Lemma we need to think about:

- the error term can be written as $O(\frac{N}{(logN)^(C-2B)}$ because B relates to$Q \leq (logN)^B$ this is why it is important that $C > 2B$ in order to get an error term that is smaller than O(N).

- the main idea of the proof is that if α is close to a rational number a/q which is in a piece of the major arc labeled by $a/q or \beta = \alpha - a/q$ has a very small value

- then we can use Lemma 8.2 to bound $|F(\alpha) - \mu(q)u(\beta)|$ if $\beta = 0 and \alpha = a/q is rational, then u(0) = N and so we get F(\alpha) = F(a/q) = \mu(q)/\phi(q)N + a smaller error which is the statment of Lemma 8.2$ this lets us generalize a small part of a neighborhood of a/q.

Next we will get the estimate for the major arc integral.
Theorem 8.4 For any positive numbers B,C, and $\epsilon with C > 2B$, the integral over the major arc is

$$\int_M F(\alpha)^3 e(-N\alpha)d\alpha = \mathfrak{S}(N)\frac{N^2}{2} + O(\frac{N^2}{(logN)^{(1-\epsilon)B}}) + O(\frac{N^2}{(logN)^{C-5B}}$$

where the implied constants depend only on $B, C, and \epsilon$
We use the information from Lemma 8.3 that this integral is a small absolute value for α in the a/q part of the major arc, so multiplying by $e(-N\alpha)$ and integrating over this part of the major arc and then adding all the (a,q) we find a small result.

$$\int_M (F(\alpha)^3 -)^3 - \frac{\mu(q)}{\phi(q)^3} u(\alpha - \frac{a}{q})^3) e(-N\alpha)d\alpha$$

So by multiplying by $e(-N\alpha)$ and integrating over this part of the major arc and then adding up over all the (a,q) we find that the result is very small. This tells us that:

$$\int_M F(\alpha)^3 e(-N\alpha)d\alpha\text{-} \int_M (F(\alpha)^3 -)^3 - \frac{\mu(q)}{\phi(q)^3} u(\alpha - \frac{a}{q})^3) e(-N\alpha)d\alpha$$

The first integral is what we want and it is equal to the second integral up to some small error, so we can work with it instead. Then we sum it over various different possibilities for (a,q). Now we can:

- $\mu(q)/\phi(q)^3$ part pulls out and then we change variables to get
- $e(-Na/q)$ factor
- In the integral we are left with $u(\beta)^3 e(-N\beta)$
- Summing and integrating we end up with the singular series $\mathfrak{S}(N) times the singular integral J(N)$
- We can estimate using Lemma 8.1

With an end result of:

$$= \mathfrak{S}(N)\frac{N^2}{2} + O(\frac{N^2}{(logN)^{1-\epsilon}B}) + O(\frac{N^2}{(logN)^{C-5B}})$$

5 Exponential sums over primes

This section is about the proof of a bound which will go into bounding the minor arc in the next section. This section will use Vaughan's identity because it is a more simplified version of using sieve methods. This section is quite technical so I will go over the main ideas which are:

- The main result of this section is the estimate for the exponential sum $F(\alpha)$ by using the sums S_1, S_2, S_3
- To do this we use Vaughan's identity and define it as it is more simple than using sieve methods
- Then we use this identity to get the three sums S_1, S_2, S_3

Lemma 8.4 Vaughan's identity, For $u \geq 1$, Let

$$M_u(k) = \sum_{d|\ell} d \leq u\mu(d)$$

Let $\Phi(k, \ell)$ be an arithmetic function of two variables. Then

$$\sum_{u<\ell\leq N} \Phi(1,\ell) + \sum_{u<k\leq N} \sum_{u<\ell\leq \frac{N}{\ell}} M_u(k)\Phi(k,\ell) = \sum_{d\leq u} \sum_{u<\ell\leq \frac{N}{d}} \sum_{m\leq \frac{N}{\ell d}} \mu(d)\Phi(dm,\ell)$$

The proof of this identity is in the book.
Then we have the exponential sum $F(\alpha) = S_1 - S_2 - S_3 + O(N_{1/2})$ which we will approximate using:

$$S_1 = \sum_{d\leq N^{2/5}} \sum_{\ell\leq \frac{N}{d}} \sum_{m\leq \frac{N}{\ell d}} \mu(d)\Lambda(\ell)e(\alpha d\ell m)$$

$$S_2 = \sum_{d\leq N^{2/5}} \sum_{\ell\leq N^{2/5}} \sum_{m\leq \frac{N}{\ell d}} \mu(d)\Lambda(\ell)e(\alpha d\ell m)$$

$$S_3 = \sum_{k>N^{2/5}} \sum_{N^{2/5}<\ell\leq \frac{N}{k}} N_{\frac{2}{5}}(k)\Lambda(\ell)e(\alpha k\ell)$$

To proof this we will apply Vaughan's identity with $u = N^{2/5}$ and $\Phi(k,\ell) = \Lambda(\ell)e(\alpha k\ell)$.
With the application of Vaughan's identity we end up with

$$S_1 \ll (\frac{N}{q} + N^{2/5} + q)(logN)^2$$

$$S_2 \ll (\frac{N}{q} + N^{4/5} + q)(logN)^2$$

$$S_3 \ll (logN)^4(\frac{N}{q^{1/2}} + N^{4/5} + q^{1/2}N^{1/2})$$

6 Proof of the asymptotic formula

The final section will assemble everything together to prove the formula.The real goal is to prove that every sufficiently large odd number can be written as the sum of three primes, $i.e.r(N)1$ for N odd and sufficiently large. To do this we will:

- first for R(N) and then deducing the formula for r(N) from it

Theorem 8.7 Vinogradov Let $\mathfrak{S}(N) bethesingularseriesfortheternaryGoldbachproblem.Forallsuf ficientlyla$
)

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

where the implied constant depends only on A.

We want to take

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

and turn it into

$$r(N) = \mathfrak{S}(N)\frac{N^2}{2(logN)^3}(1 + O(\frac{loglogN}{logN}))$$

From R(N) to r(N) we need to find the upper bound for R(N) which is

$$\ll \frac{N^{2-\delta}}{(logN)^2}$$

Now we need to get a lower bound for R(N)

$$\gg (1-\delta)^3(logN)^3(r(N) - \frac{N^{2-\delta}}{(logN)^2}$$

By setting up the inequality:

$$(logN)^3 r(N) \leq (1-\sigma)^{-3}R(N) + (logN)^{2-\sigma}$$

Then by using Theorem 8.7 we can solve for R(N) by using the fact of $R(N) \ll N^2$ which is:

$$0 \leq (logN)^3 r(N) - R(N) \leq ((q-\sigma)^{-3} - 1)R(N) + (logN)N^{2-\sigma} \text{ which deduces to } N^2(\sigma + \frac{logN}{N^\sigma})$$

Now we will deduce this equation to find r(N).

Then we find the value of σ that makes the equation hold which is:

$$\sigma = \frac{2loglogN}{logN}$$

Plug this into the same inequality as before:

$$0 \leq (logN)^3 r(N) - R(N) \ll \frac{N^2 loglogN}{logN}$$

Then by using Theorem 8.7 again we are able to solve for r(N).

$$r(N) = \mathfrak{S}(N)\frac{N^2}{2(logN)^3}(1 + O(\frac{loglogN}{logN}))$$

The important take away is that the real goal is to prove that every sufficiently large odd number can be written as the sum of three primes or $r(N) \geq 1 for N odd and suf ficiently large$. Here they focus on the precise formula for r(N), but to prove this we can also show that R(N) goes to infinity.