VINOGRADOV'S THREE PRIME THEOREM

NICHOLAS ROUSE

ABSTRACT. I sketch Vinogradov's 1937 proof that every sufficiently large odd integer is the sum of three prime numbers. The result is dependent on numerous intermediate results, some of which I prove and others of which have proofs too long to give here. The main technique is decomposition into major and minor arcs.

CONTENTS

1. THE VON MANGOLDT FUNCTION AND COUNTING REPRESENTATIONS

Definition 1.1. We define the von Mangoldt function as

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^k \text{ for a prime number } p, \\ 0 & \text{otherwise.} \end{cases}$$

The motivation for introducing this function is another function.

Definition 1.2.

$$r(n) = \sum_{k_1+k_2+k_3=n} \Lambda(k_1)\Lambda(k_2)\Lambda(k_3).$$

The function $r(n)$ is the number of ways to express n as the sum of three numbers that each are either prime or a power of a prime number with weight of $\log(p_1)\log(p_2)\log(p_3)$ attached to that value. Clearly, if there are no representations of a given integer (in our case, we shall be interested in odd integers) as the sum of three prime numbers, then $r(n) = 0$. However, $r(n) \neq 0$ does not guarantee that such a representation exists, only that one of prime powers does. However, from partial summation we can see that the prime powers contribute less than the actual prime numbers, so a bound on $r(n)$ will be sufficient.

Date: August 30, 2013.

2. A first bound

Consider the sum
$$S(\alpha) = \sum_{k \le N} \Lambda(n) e^{2\pi k i \alpha},$$
for some arbitrary constants n and N. We can recover something resembling $r(n)$ if we take the cube of the sum
$$S(\alpha)^3 = \sum_{k_1,k_2,k_3 \le N} \Lambda(k_1)\Lambda(k_2)\Lambda(k_3) e^{2\pi(k_1+k_2+k_3)i\alpha}.$$
This looks similar to $r(n)$ but there is the issue that k_1, k_2, and k_3 are each less than a constant N rather than their sum equal to another constant n. We will decompose the sum so that k_1, k_2 and $k_3 = n$ is part of the sum.
$$S(\alpha)^3 = \sum_n \left(\sum_{\substack{k_1+k_2+k_3=n \\ k_1,k_2,k_3 \le N}} \Lambda(k_1)\Lambda(k_2)\Lambda(k_3) \right) e^{2\pi n i \alpha}.$$
Again, this is not quite $r(n)$ because if $n > N$, the inner sum will not necessarily count all representations (appropriately weighted, of course). However, this is not really an issue as we can denote the inner sum $r(n, N)$ and point out that it is identical to $r(n)$ for $n \le N$, so we'll write $S(\alpha)^3$ as
$$S(\alpha)^3 = \sum_n r(n,N) e^{2\pi n i \alpha}.$$
We have a Fourier series, so we can find the coefficients of the Fourier series
$$r(n) = \int_{\mathbb{R}/\mathbb{Z}} S(\alpha)^3 e^{-2\pi n i \alpha} d\alpha, \tag{2.1}$$
where $\mathbb{R}/\mathbb{Z}$ is the quotient group of the real numbers modulo the integers. As a brief remark, $\mathbb{R}/\mathbb{Z}$ is isomorphic to the unit circle, so the integral can be understood as integrating over the circle. Appropriately, the technique of setting up such an integral is called the Hardy-Littlewood circle method. There is no obvious way to bound this integral, but the approach of Vinogradov is to consider the integral over subintervals of $\mathbb{R}/\mathbb{Z}$. The subintervals are the major arcs (denoted $\mathfrak{M}$) and the minor arcs (denoted $\mathfrak{m}$). Intuitively, the major arcs are the subintervals near a rational number with a small denominator. Minor arcs are everything else in $\mathbb{R}/\mathbb{Z}$. We will define major and minor arcs more precisely.

3. Some definitions

Definition 3.1. For constants n and B, let $P = \log^B(n)$ and $Q = n/\log^{2B}(n)$. For any $q \le P$ and a such that $1 \le a \le q$ where the greatest common divisor of a and q (henceforth denoted (a,q)) is 1, we define
$$\mathfrak{M}(a,q) = \{\alpha \in \mathbb{R}/\mathbb{Z} \mid \left|\alpha - \frac{a}{q}\right| \le \frac{1}{Q}\}.$$
Moreover, let $\mathfrak{M}$ be the union of all such $\mathfrak{M}(a,q)$ and $\mathfrak{m}$ be the complement of $\mathfrak{M}$ in $\mathbb{R}/\mathbb{Z}$.

Lemma 3.2. $\mathfrak{m}$ *is nonempty.*

Proof. Any two major arcs are disjoint. To prove this, we take $\frac{a}{q} \neq \frac{a'}{q'}$ Then we have for sufficiently large N

$$\left|\frac{a}{q} - \frac{a'}{q'}\right| \geq \frac{1}{qq'} \geq \frac{1}{P^2} > \frac{2}{Q}.$$

Since the major arcs are then not all of $\mathbb{R}/\mathbb{Z}$, $\mathfrak{m}$ is nonempty. □

If we can bound (2.1) when integrating over the major and minor arcs individually, we will succeed in bounding the whole integral. For the sake of exposition, however, we will first state some basic definitions from group theory and analytic number theory for objects we will use.

Definition 3.3. For integers a and q, the congruence class or residue class of a mod q is denoted as $\bar{a}_q$ and defined as

$$\overline{a}_q = \{a + kn \mid k \in \mathbb{Z}\}.$$

Moreover, the integer a is said to be the representative integer or simply the representative for the residue class.

Definition 3.4. The integers modulo q (denoted $\mathbb{Z}/q\mathbb{Z}$) is the set of all congruence classes a mod q. That is

$$\mathbb{Z}/q\mathbb{Z} = \{\overline{a}_q \mid a \in \mathbb{Z}\}.$$

Definition 3.5. A Dirichlet character to modulus q is any function $\chi : \mathbb{Z} \to \mathbb{C}$ with the following properties:

(1) If p and q are not relatively prime, then $\chi(p) = 0$. That is, if $(p, q) \neq 1$, $\chi(p) = 0$.
(2) If $(p, q) = 1$, then $|\chi(p)| = 1$.
(3) If q_1 and q_2 are any two positive integers, then $\chi(q_1 q_2) = \chi(q_1)\chi(q_2)$.

If $q = 1$, the Dirichlet character is called the trivial character and denoted χ_0. A Dirichlet character χ is called primitive modulo q if for every divisor d of q there exists an integer $x \equiv 1 \mod d$ and $(x, q) = 1$, such that $\chi(x) \neq 1$. Moreover, the set of all Dirichlet characters modulo q is denoted $\widehat{\mathbb{Z}/q\mathbb{Z}}$.

4. Working with major arcs

We start with an individual $\mathfrak{M}(a, q)$. For any character χ to modulus q, we can consider the Gauss sum

$$\tau(\chi) = \sum_{m \in \mathbb{Z}/q\mathbb{Z}} \chi(m) e^{2\pi i m/q}.$$

We can consider another sum

$$\frac{1}{\phi(q)} \sum_{\chi \in \widehat{\mathbb{Z}/q\mathbb{Z}}} \chi(n)\tau(\overline{\chi}),$$

where $\phi(q)$ is the Euler totient function and is equal to the number of positive integers less than or equal to q such that $(n, q) = 1$ and $\overline{\chi}$ is simply the complex conjugate of the Dirichlet character. By the first property of definition 3.5 we have,

$$\frac{1}{\phi(q)} \sum_{\chi \in \widehat{\mathbb{Z}/q\mathbb{Z}}} \chi(n)\tau(\overline{\chi}) = 0 \qquad \text{if } (n, q) \neq 1.$$

However, if $(n,q)=1$, then we have from the Gauss sum,

$$\frac{1}{\phi(q)}\sum_{\chi\in\widehat{\mathbb{Z}/q\mathbb{Z}}}\chi(n)\tau(\overline{\chi})=\frac{1}{\phi(q)}\sum_{\chi\in\widehat{\mathbb{Z}/q\mathbb{Z}}}\sum_{m\in\mathbb{Z}/q\mathbb{Z}}\chi(n)\overline{\chi}(m)e^{2\pi i m/q}.$$

If we take $m\equiv nh \bmod q$ we then have,

$$\frac{1}{\phi(q)}\sum_{\chi\in\widehat{\mathbb{Z}/q\mathbb{Z}}}\sum_{m\in\mathbb{Z}/q\mathbb{Z}}\chi(n)\overline{\chi}(m)e^{2\pi i m/q}=\frac{1}{\phi(q)}\phi(q)\sum_{\chi\in\widehat{\mathbb{Z}/q\mathbb{Z}}}\sum_{m\in\mathbb{Z}/q\mathbb{Z}}\overline{\chi}(h)e^{2\pi i n h/q}$$

$$=\frac{1}{\phi(q)}\sum_{h\in\mathbb{Z}/q\mathbb{Z}}e^{2\pi i n h/q}\sum_{\chi\in\widehat{\mathbb{Z}/q\mathbb{Z}}}\overline{\chi}(h)$$

$$=e^{2\pi n/q}.$$

Then we have,

$$e^{2\pi n/q}=\frac{1}{\phi(q)}\sum_{\chi\in\widehat{\mathbb{Z}/q\mathbb{Z}}}\chi(n)\tau(\overline{\chi}). \tag{4.1}$$

We return to the function $S(\alpha)$ and take $\alpha=a/q+\beta$

$$S(\alpha)=\sum_{\substack{k\leq N\\(k,q)=1}}\Lambda(k)e^{2\pi k i(a/q+\beta)}+O(\log^2(N)).$$

The error term accounts for fact that this sum restricts $S(\alpha)$ to k values such that $(k,q)=1$. At any rate, we can manipulate this sum using (4.1)

$$S(\alpha)=\frac{1}{\phi(q)}\sum_{k\leq N}\Lambda(k)\sum_{\chi\in\widehat{\mathbb{Z}/q\mathbb{Z}}}\chi(ka)\tau(\overline{\chi})e^{2\pi i k\beta}+O(\log^2(N))$$

$$=\frac{1}{\phi(q)}\sum_{\chi\in\widehat{\mathbb{Z}/q\mathbb{Z}}}\tau(\overline{\chi})\chi(a)\sum_{k\leq N}\chi(k)\Lambda(k)e^{2\pi i k\beta}+O(\log^2(N)).$$

Here we can use summation by parts

$$\sum_{k\leq N}\chi(k)\Lambda(k)e^{2\pi i k\beta}=e^{2\pi i N\beta}\sum_{n\leq N}\chi(n)\Lambda(n)-2\pi i\beta\int_1^N e^{2\pi i u\beta}\sum_{n\leq u}\chi(n)\Lambda(n)du. \tag{4.2}$$

We introduce $\psi(x,\chi)$, which we define as

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

We can rewrite (4.2) as

$$\sum_{k\leq N}\chi(k)\Lambda(k)e^{2\pi i k\beta}=e^{2\pi i N\beta}\psi(N,\chi)-2\pi i\beta\int_1^N e^{2\pi i u\beta}\psi(u,\chi)du. \tag{4.3}$$

We have reached the first very important lemma.

Lemma 4.4. *Let χ be a nontrivial Dirichlet character to modulus q. If $q \leq \log^M(x)$ for a positive constant M, then*

$$\left|\psi(x,\chi)\right| = O(xe^{-C(M)\sqrt{\log(x)}}),$$

for a positive constant $C(M)$ which is a function of solely M.

This lemma is actually equivalent to the prime number theorem for arithmetic progressions. This lemma is the first but not last result whose proof I must omit for space considerations. We can apply the lemma to (4.3) to obtain a bound for the nontrivial Dirichlet characters.

$$\sum_{k\leq N} \chi(k)\Lambda(k)e^{2\pi ik\beta} = O((1+|\beta|\,N)Ne^{-c\sqrt{\log(N)}}).$$

However, our lemma does not treat the contribution from the trivial Dirichlet character. We can work with another ψ function (this one is known as the summatory von Mangoldt function or the second Chebyshev function).

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

Note that

$$\chi_0 = \begin{cases} 1 & \text{if } (n,q)=1 \\ 0 & \text{if } (n,q)\neq 1 \end{cases}.$$

Then we have that

$$\left|\psi(x,\chi_0) - \psi(x)\right| \leq \sum_{\substack{n\leq x \\ (n,q)>1}} \Lambda(n) = O(\log(q)\log(x)).$$

The prime number theorem gives us an additional bound for $\psi(x)$,

$$\psi(x) = x + O(xe^{-c\sqrt{\log(x)}}).$$

We can set $\psi(u,\chi_0) = \lfloor u \rfloor + R(u)$ to obtain

$$R(u) = O(ue^{-c\sqrt{\log(u)}}). \tag{4.5}$$

We define another function

$$T(\beta) = \sum_{1\leq k\leq N} e^{2\pi ik\beta}.$$

We again use summation by parts to obtain

$$T(\beta) = e^{2\pi iN\beta} - 2\pi iN\beta \int_1^N e^{2\pi iN\beta}\lfloor u \rfloor du.$$

Applying this result to (4.2), we have

$$\sum_{k\leq N} \chi_0(k)\Lambda(k)e^{2\pi ik\beta} = T(\beta) + e^{2\pi iN\beta}R(N) - 2\pi i\beta \int_1^N e^{u\beta}R(u)du.$$

We use (4.5) to get

$$T(\beta) + e^{2\pi iN\beta}R(N) - 2\pi i\beta \int_1^N e^{u\beta}R(u)du = T(\beta) + O((1+|\beta|\,N)Ne^{-c\log(N)}).$$

So it is clear that the sum for the trivial Dirichlet character differs from the sum for nontrivial Dirichlet characters given by the lemma by only the term $T(\beta)$. We can combine the contributions from both the trivial and nontrivial Dirichlet characters to obtain

(4.6)
$$S(\alpha)=\frac{1}{\phi(q)}\left(\tau(\chi_0)T(\beta)+O((1+|\beta|\,N)Ne^{-c\sqrt{\log(N)}})+\sum_{\substack{\chi\in\mathbb{Z}/q\mathbb{Z}\\ \chi\neq\chi_0}}\tau(\overline{\chi})\chi(a)\left(O(1+|\beta|\,N)Ne^{-c\sqrt{\log(N)}}\right)\right).$$

That is an estimate, but two facts about Gauss sums will improve it. First, we need a definition.

Definition 4.7. The Möbius function $\mu:\mathbb{N}\to\{-1,0,1\}$ is defined as

$$\mu(q)=\begin{cases}1 & \text{if q is not divisible by a perfect square and has an even number of prime factors,}\\ -1 & \text{if q is not divisible by a perfect square and has an odd number of prime factors,}\\ 0 & \text{if q is divisible by a perfect square.}\end{cases}$$

Lemma 4.8. *Let $\tau(\chi_0)$ be a Gauss sum and $\mu(q)$ be the Möbius function, then*

$$\tau(\chi_0)=\mu(q).$$

Proof.

$$\tau(\chi_0)=\sum_{m=1}^{q}\chi_0(m)e^{2\pi im/q}=\sum_{\substack{m\leq q\\ (m,q)=1}}e^{2\pi im/q}.$$

Setting $m'd=m$ we have

$$=\sum_{d=1}^{q}\mu(d)\sum_{1\leq m'\leq q/d}e^{2\pi im'd/q}=\mu(q).$$

□

Lemma 4.9. *Let $\tau(\chi_0)$ be a Gauss sum, then*

$$\left|\tau(\chi)\right|\leq\sqrt{q}.$$

Proof. We will prove this fact for primitive Dirichlet characters and omit the longer proof regarding imprimitve characters. Taking χ primitive we have

$$\chi(n)\tau(\overline{\chi})=\sum_{h\in\mathbb{Z}/q\mathbb{Z}}\overline{\chi}(h)e^{2\pi inh/q}.$$

We can consider the square.

$$\sum_{n\in\mathbb{Z}/q\mathbb{Z}}\left|\chi(n)\right|^2\left|\tau(\overline{\chi})\right|^2=\sum_{h_1\in\mathbb{Z}/q\mathbb{Z}}\sum_{h_2\in\mathbb{Z}/q\mathbb{Z}}\overline{\chi}(h_1)\chi(h_2)\sum_{n\in\mathbb{Z}/q\mathbb{Z}}e^{2\pi i(h_1-h_2)n/q}.$$

So then we have that

$$\phi(q)\left|\tau(\overline{\chi})\right|^2=q\sum_{h\in\mathbb{Z}/q\mathbb{Z}}\left|\chi(h)\right|^2=q\phi(q),$$

and it follows that

$$\left|\tau(\chi)\right|\leq\sqrt{q}.$$

□

With these two facts, we can significantly clean up (1.5) to obtain

$$S(\alpha) = \frac{\mu(q)}{\phi(q)}T(\beta) + O((1+|\beta|\,N)\sqrt{q}Ne^{-c\sqrt{\log(N)}}).$$

Returning to the definition of major arcs, we can set $q \leq P$ and $|\beta| \leq \frac{1}{Q}$ because α is in the major arc $\mathfrak{M}(a,q)$. So we have

$$S(\alpha) = \frac{\mu(q)}{\phi(q)}T\beta + O(Ne^{-c\sqrt{\log(N)}}).$$

If we take the cube, we can return to the Fourier series that we are interested in.

$$\int_{\mathfrak{M}(a,q)} S\alpha^3 e^{-2\pi i N\alpha} d\alpha = \frac{\mu(q)}{\phi(q)^3}e^{-2\pi i aN/q}\int_{-1/Q}^{1/Q} T(\beta)^3 e^{-2\pi i N\beta} d\beta + O(N^2 e^{-c'\sqrt{\log(N)}}).$$

The c' merely accounts for the possibility that there is different constant here. This integral accounts for a single major arc. If we want to find the contribution of all the major arcs, we will have to sum over all of them.

$$\int_{\mathfrak{M}} S\alpha^3 e^{-2\pi i N\alpha} d\alpha = \sum_{q\leq P}\frac{\mu(q)}{\phi(q)^3}\left(\sum_{\substack{a=1\\(a,q)=1}}^{q} e^{2\pi i aN/q}\right)\int_{-1/Q}^{1/Q} T(\beta)^3 e^{-2\pi i N\beta} d\beta + O(N^2 e^{-c''\sqrt{\log(N)}}).$$

The sum

$$\left(\sum_{\substack{a=1\\(a,q)=1}}^{q} e^{2\pi i aN/q}\right).$$

is called Ramanujan's sum and is denoted c_q. We now make a detour into some important definitions and results from number theory. The penultimate proof must be omitted for space, but all others will be supplied.

Definition 4.10. An arithmetic function is a function $f : \mathbb{N} \to \mathbb{C}$. Moreover, we define addition for arithmetic functions f and g as

$$(f+g)(n) = f(n) + g(n).$$

Definition 4.11. An arithmetic function f is multiplicative if $f(mn) = f(m)f(n)$ whenever $(m,n) = 1$

Lemma 4.12. *If f is a multiplicative function of n and*

$$\lim_{p^k\to\infty} f(p^k) = 0,$$

where p^k is a prime power (so the limit goes through all prime powers), then

$$\lim_{n\to\infty} f(n) = 0.$$

Proof. The hypothesis implies that there are only finitely many prime powers such that $\left|f(p^k)\right| \geq 1$. We define

$$A = \prod_{\left|f(p^k)\right|\geq 1} \left|f(p^k)\right|.$$

Clearly, $A \geq 1$. Choose ϵ such that $0 < \epsilon < A$. Then there are only finitely many prime powers such that $\left|f(p^k)\right| \geq \epsilon/A$. If we consider a fixed p^k that divides an integer n, there will only be finitely many integers n such that $\left|f(p^k)\right| \geq \epsilon/A$. It follows that if n is sufficiently large, there is at least one prime power p^k that divides n and $\left|f(p^k)\right| < \epsilon/A$. Take $p_1, ..., p_{r+s+t}$ as pairwise distinct primes with the following properties

(1) $1 \leq \left|f(p_i^{k_i})\right|$ for $i = 1, ..., r$.
(2) $\epsilon/A \leq \left|f(p_i^{k_i})\right| < 1$ for $i = r+1, ..., r+s$.
(3) $\left|f(p_i^{k_i})\right| < \epsilon/A$ for $i = r+s+1, ..., r+s+t$.
(4) $t \geq 1$.

We can write n as

$$n = \prod_{i=1}^{r} p_i^{k_i} \prod_{i=r+1}^{r+s} p_i^{k_i} \prod_{i=r+s+1}^{r+s+t} p_i^{k_i}.$$

Then we have

$$\left|f(n)\right| = \prod_{i=1}^{r} \left|f(p_i^{k_i})\right| \prod_{i=r+1}^{r+s} \left|f(p_i^{k_i})\right| \prod_{i=r+s+1}^{r+s+t} \left|f(p_i^{k_i})\right| < A(\epsilon/A)^t \leq \epsilon.$$

□

Lemma 4.13. *For $\epsilon > 0$ and sufficiently large n,*

$$n^{1-\epsilon} < \phi(n) < n.$$

Proof. Clearly, if $n > 1$, then $\phi(n) < n$, and for prime number p, $\frac{p}{p-1} \leq 2$, so we have

$$\frac{p^{m(1-\epsilon)}}{\phi(p^m)} = \frac{p^{m(1-\epsilon)}}{p^m - p^{m-1}} = \frac{p}{p-1}\left(\frac{p^{m(1-\epsilon)}}{p^m}\right) \leq \frac{2}{p^{m\epsilon}}.$$

It follows that

$$\lim_{p^m \to \infty} \frac{p^{m(1-\epsilon)}}{\phi(p^m)} = 0.$$

We point out that $\frac{n^{1-\epsilon}}{\phi(n)}$ is multiplicative and invoke Lemma 4.11 to obtain

$$\lim_{n \to \infty} \frac{n^{1-\epsilon}}{\phi(n)}.$$

□

Lemma 4.14. *Let*

$$c_q = \sum_{\substack{a=1 \\ (a,q)=1}}^{q} e^{2\pi i a N/q}.$$

(1) c_q is multiplicative in q.
(2) If, for p prime, p^α is the highest power of p that divides n, then

$$c_{p^\beta}(n) = \begin{cases} \phi(p^\beta) & \text{if } \beta \leq \alpha, \\ -p^\alpha & \text{if } \beta = \alpha + 1, \\ 0 & \text{if } \beta > \alpha + 1. \end{cases}$$

Lemma 4.15. *Let*

$$\mathfrak{G}(N) = \sum_{q=1}^{\infty} \frac{\mu(q)c_q(n)}{\phi(q)^3}.$$

$\mathfrak{G}(N)$ converges absolutely and uniformly in N and has Euler product

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

Moreover, there exist positive constants c_1 and c_2 such that for all positive odd N

$$c_1 < \mathfrak{G}(N) < c_2.$$

Proof. Clearly we have $c_q(N) < \phi(n)$. For positive ϵ and sufficiently large q, by Lemma 4.12, we have

$$\frac{\mu(q)c_q(n)}{\phi(q)^3} < \frac{1}{\phi(q)^2} < \frac{1}{q^{2-\epsilon}}.$$

So $\mathfrak{G}(N)$ converges absolutely and uniformly in N. Moreover, using Lemma 4.13 with $\beta = 1$, we have

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

Since the Möbius function, the Euler totient function, and Ramanujan's sum are all multiplicative, we can evaluate the Euler product for $\mathfrak{G}(N)$.

$$\mathfrak{G}(N) = \prod_p \left(1 + \sum_{j=1}^{\infty} \frac{\mu(p^j)c_{p^j}(N)}{\phi(p^j)^3}\right) = \prod_p \left(1 - \frac{c_p(N)}{\phi(p)^3}\right)$$
$$= \prod_{p|N}\left(1 - \frac{1}{(p-1)^2}\right)\prod_{p\nmid N}\left(1 + \frac{1}{(p-1)^3}\right).$$

It follows that for all $N > 0$ there exist c_1 and c_2 such that $c_1 < \mathfrak{G}(N) < c_2$. As an observation, note that $\mathfrak{G}(N) = 0$ when N is even. ☐

We can use this estimate to bound another part of the sum.

$$\sum_{q>P} \frac{\mu(q)c_q(n)}{\phi(q)^3} = O\left(\sum_{q>p} \frac{1}{\phi(q)^2}\right) = O(\log^{-B+1}(N)),$$

where B is a constant that we will choose later. We can combine these two results to bound the sum that actually appears in the integral over the major arcs.

$$\sum_{q \le P} \frac{\mu(q)c_q(N)}{\phi(q)^3} = \mathfrak{G}(N) + O(\log^{-B+1}(N)). \tag{4.16}$$

We have obtained suitable bounds for a term in the integral over the major arcs, but we still have to treat another term. We will do this by splitting the integral into an integral with more tractable limits of integration and a term we can bound more easily.

$$\int_{-1/Q}^{1/Q} T(\beta)^3 e^{-2\pi i N\beta} d\beta = \int_0^1 T(\beta)^3 e^{-2\pi i N\beta} d\beta + O\left(\int_{1/Q}^{1-1/Q} \left|T(\beta)^3\right| d\beta\right).$$

We invoke that we defined $T(\beta)$ as a geometric series and can evaluate it as such. We define $||x||_{\mathbb{R}/\mathbb{Z}}$ as the distance between x and the nearest integer.

$$T(\beta) = \frac{e^{2\pi i((N+1)B)} - e^{2\pi i\beta}}{e^{2\pi i\beta} - 1} = O(\min\left(N, \frac{1}{||\beta||_{\mathbb{R}/\mathbb{Z}}}\right)).$$

We can evaluate the rightmost term.

$$\int_{-1/Q}^{1/Q} T(\beta)^3 e^{-2\pi i N\beta} d\beta = \int_0^1 T(\beta)^3 e^{-2\pi i N\beta} d\beta + O(Q^2).$$

We express Q in terms of N as in the definition of major arcs.

$$\int_0^1 T(\beta)^3 e^{-2\pi i N\beta} d\beta + O(Q^2) = \int_0^1 T(\beta)^3 e^{-2\pi i N\beta} d\beta + O\left(\frac{N^2}{\log^{4B}(N)}\right).$$

The remaining integral counts representations of N as the sum of three positive integers. So we can have a bound for it.

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

Combining these results we have a complete bound for the integral.

$$\int_{-1/Q}^{1/Q} t(\beta)^3 e^{-2\pi i N\beta} d\beta = \frac{N^2}{2} + O\left(\frac{N^2}{\log^{4NB}(N)}\right). \tag{4.17}$$

Combining results we obtain a desirable bound for the integral over the major arcs.

$$\int_{\mathfrak{M}} S(\alpha)^3 e^{-2\pi i N\alpha} d\alpha = \frac{1}{2}\mathfrak{G}(N)N^2 + O\left(\frac{N^2}{\log^{B-1}(N)}\right). \tag{4.18}$$

5. The minor arcs

As the name perhaps implies, the minor arcs are less important than the major ones. In fact, Vinogradov's theorem relies on the minor arcs contributing sufficiently small amounts that the major arcs dominate. The integral we must consider then is over the minor arcs. We can begin with some straightforward bounds.

$$\left|\int_{\mathfrak{m}} S(\alpha)^3 e^{-2\pi i N\alpha} d\alpha\right| \leq \left(\max_{\mathfrak{m}} |S(\alpha)|\right) \int_{\mathfrak{m}} \left|S(\alpha)^2\right| d\alpha.$$

Of course, the whole interval $[0, 1]$ will contribute more on the integral than just the minor arcs, so we can bound the integral over the minor arcs above with that interval and obtain a more workable integral.

$$\left(\max_{\mathfrak{m}} |S(\alpha)|\right) \int_{\mathfrak{m}} \left|S(\alpha)^2\right| d\alpha \leq \left(\max_{\mathfrak{m}} |S(\alpha)|\right) \int_0^1 \left|S(\alpha)^2\right| d\alpha.$$

We can treat this integral using the definition of $S(\alpha)$.

$$\int_0^1 \left|S\alpha^2\right| d\alpha = \sum_{k_1 \leq N} \Lambda(k_1) \sum_{k_2 \leq N} \Lambda(k_2) \int_0^1 e^{2\pi i\alpha(k_1 - k_2)} d\alpha.$$

Taking $k_1 = k_2 = k$ we have a bound.

$$\sum_{k_1 \leq N} \Lambda(k_1) \sum_{k_2 \leq N} \Lambda(k_2) \int_0^1 e^{2\pi i\alpha(k_1 - k_2)} d\alpha = \sum_{k \leq N} \Lambda(k)^2 = O(N\log(N)). \tag{5.1}$$

We have to consider $\max_{\mathfrak{m}} \left|S(\alpha)\right|$. We will start by working with the definition of minor arc. Take $\alpha \in \mathfrak{m}$ and $q \leq P$.

$$\left|\alpha - \frac{a}{q}\right| > \frac{1}{Q} = \frac{\log^{2B}(N)}{N}.$$

We can generalize to a statement about all elements of the minor arcs.

$$\inf_{1 \leq q \leq P} \left|\alpha - \frac{a}{q}\right| > \frac{\log^{2B}(N)}{N}. \tag{5.2}$$

We are in need of the last lemma whose proof is too lengthy to give here.

Lemma 5.3. *For $\alpha \in \mathbb{R}$, $C > 0$, fixed k, and sufficient large N, if*

$$\inf_{1 \leq d \leq 16 \log^{8(C+4)(N)}} ||d\alpha||_{\mathbb{R}/\mathbb{Z}} \geq k \frac{\log^{28(C+4)}(N)}{N},$$

then

$$\left|\frac{1}{N} \sum_{1 \leq n \leq N} \mu(n) e^{2\pi i n \alpha}\right| = O(\log^{-C+1}(N)).$$

The statement of the lemma involves the Möbius function. We will have to manipulate it to work with the von Mangoldt function. We can work with the definitions of these two functions.

$$\Lambda(n) = \sum_{d|n} \log(d) \mu\left(\frac{n}{d}\right).$$

The Möbius function is not defined on values other than the natural numbers, but we can fill in the function by taking $\mu(x) = 0$ when $x \notin \mathbb{N}$. We can rewrite the von Mangoldt function in terms of this new Möbius function.

$$\Lambda(n) = \sum_{d \leq n} \log(d) \mu\left(nd\right).$$

We can rewrite $S(\alpha)$.

$$S(\alpha) = \sum_{n \leq N} \Lambda(n) e^{2\pi i n \alpha}.$$

Note that this is simply the original definition of $S(\alpha)$. We replace the von Mangoldt function with the Möbius function.

$$\sum_{n \leq N} \Lambda(n) e^{2\pi i n \alpha} = \sum_{n \leq N} \sum_{d \leq n} \log(d) \mu\left(\frac{n}{d}\right) e^{2\pi i n \alpha}.$$

We define $m = \frac{n}{d}$ and further manipulate the sum.

$$\sum_{n \leq N} \sum_{d \leq n} \log(d) \mu\left(\frac{n}{d}\right) e^{2\pi i n \alpha} = \sum_{d \leq N} \log(d) \sum_{m \leq \frac{N}{d}} \mu(m) e^{2\pi i m d \alpha}.$$

We transform (5.2) to something that resembles the conditions on the lemma by considering the distance from $q\alpha$ to the nearest integer.

$$\inf_{1 \leq q \leq \log^B(N)} ||q\alpha||_{\mathbb{R}/\mathbb{Z}} > \frac{\log^{4B}(N)}{N}.$$

We can recover the conditions on the lemma with $B = 9(C+4)$. We can bound $S(\alpha)$ in the minor arcs.

$$S(\alpha) < \sum_{d \le N} \log(d) \frac{N/d}{\log^{\frac{B}{9}-5}(N/d)}$$

$$\le \frac{1}{\log^{\frac{B}{9}-6}(N)} \sum_{d \le N} \frac{N}{d} = O\left(\frac{N}{\log^{\frac{B}{9}-6}(N)}\right).$$

We can bring this bound with (5.1) to obtain a bound over the minor arcs.

$$\int_{\mathfrak{m}} S(\alpha)^3 e^{-2\pi i N\alpha} d\alpha = O\left(\frac{N^2}{\log^{\frac{B}{9}-6}(N)}\right). \tag{5.4}$$

6. Vinogradov's Theorem

We can combine these results into Vinogradov's theorem.

Theorem 6.1. *For $A > 0$,*

$$r(n) = \frac{1}{2}\mathfrak{G}(N)N^2 + O\left(\frac{N^2}{\log^A(N)}\right).$$

Proof. From (2.1) we have

$$r(n) = \int_{\mathbb{R}/\mathbb{Z}} S(\alpha)^3 e^{-2\pi n i\alpha} d\alpha.$$

From major and minor arc decomposition, we split the integral obtaining,

$$\int_{\mathbb{R}/\mathbb{Z}} S(\alpha)^3 e^{-2\pi n i\alpha} d\alpha = \int_{\mathfrak{M}} S(\alpha)^3 e^{-2\pi n i\alpha} d\alpha + \int_{\mathfrak{m}} S(\alpha)^3 e^{-2\pi n i\alpha} d\alpha.$$

From (4.14), we have

$$\int_{\mathfrak{M}} S(\alpha)^3 e^{-2\pi i N\alpha} d\alpha = \frac{1}{2}\mathfrak{G}(N)N^2 + O\left(\frac{N^2}{\log^{B-1}(N)}\right).$$

From (5.4) we have

$$\int_{\mathfrak{m}} S(\alpha)^3 e^{-2\pi i N\alpha} d\alpha = O\left(\frac{N^2}{\log^{\frac{B}{9}-6}(N)}\right).$$

We take $B = 9(A+6)$, and note that the power on the logarithm is much smaller in the denominator of the error term from the minor arcs than that from the major arcs, so we have

$$r(n) = \int_{\mathfrak{M}} S(\alpha)^3 e^{-2\pi n i\alpha} d\alpha + \int_{\mathfrak{m}} S(\alpha)^3 e^{-2\pi n i\alpha} d\alpha = \frac{1}{2}\mathfrak{G}(N)N^2 + O\left(\frac{N^2}{\log^A(N)}\right).$$

□

Corollary 6.2. *Every sufficiently large odd integer is the sum of three primes.*

Proof. By Lemma 4.14 $\mathfrak{S}(N)$ is bounded for all odd N, so for sufficiently large N, N^2 is much greater than $\mathfrak{S}(N)$, so $r(n)$, the number of representations of n as the sum of three prime powers, is bounded below for sufficiently large N. Moreover, we can see by partial summation that the contribution from sums of proper prime powers is much less than that of prime numbers. Therefore, for sufficiently large values of N, N has a representation as the sum of three prime numbers. □

Acknowledgments. This paper would not have been possible without the help of my mentor Mohammad Rezaei. Not only did he make me aware of the theorem this paper covers, but he guided me to the middle path away from a paper that would have been too simple by assuming the Generalized Riemann Hypothesis and a paper that would be five times as long as the present one if I had attempted to prove all of the results stated. Moreover, Mohammad was invaluable in answering questions about this paper. As far as written mathematical sources go, this paper largely follows the path set by Ian Petrow, the first source in the bibliography. Supplemental material about number theory is mostly from the next two sources, Nathanson and Apostol. The remaining three web sources were useful in understanding the methods and steps featured in Petrow's paper. Of course, it would not do not to thank Peter May for his efforts in running the REU that allowed me to spend my summer doing mathematics.

References

[1] Ian N Petrow. Vinogradov's Three Primes Theorem. http://math.stanford.edu/ ipetrow/V3.pdf.
[2] Melvyn B. Nathanson. Additive Number Theory: The Classical Bases. Springer. 1996.
[3] Tom M. Apostol. Introduction to Analytic Number Theory. Springer-Verlag. 1976.
[4] Noah Snyder. Dirichlet L-functions, Dirichlet Characters and primes in arithmetic progressions. http://math.columbia.edu/ nsnyder/tutorial/lecture2.pdf.
[5] Andreas Strömnergsson. Analytic Number Theory: Lecture Notes Based on Davenport's Book. http://www2.math.uu.se/ astrombe/analtalt08/www_notes.pdf.
[6] Andreas Strömnergsson. Applications of the Hardy-Littlewood Circle Method. http://home.wlu.edu/ baczkowskid/talks/number_theory/waring3.pdf.