Proof of Vinogradov's Three Primes Theorem

by David Rhee

We will discuss the proof of the Vinogradov's Three Primes Theorem, assuming that the generalized Riemann Hypothesis is true. The theorem says the following:

Let N be a sufficiently large odd number. Then N can be written as a sum of three primes.

1. **Definitions and Properties**

   (a) Defintion) $e(q) = e^{2\pi i q}$

   (b) Euler's totient function

   Defintion) $\phi(n)$ is the number of integers in $[1, n]$ that are coprime to n.

   - $\phi(q)$ is multiplicative (i.e. $\phi(nm) = \phi(n)\phi(m)$ if $(n, m) = 1$).
   - $\phi(q) \gg q/\log q$

   (c) Von Mangoldt function

   Definition) $\Lambda(n) = \begin{cases} \log p & \text{if } n = p^k \text{ for some prime } p \text{ and integer } k \geq 1, \\ 0 & \text{otherwise.} \end{cases}$

   - $\log n = \sum_{d \mid n} \Lambda(d)$
   - $\sum_{n \leq N} \Lambda(n)^2 \ll N \log N$

   (d) Dirichlet character

   Definition) Dirichlet character is a homomorphism from $\mathbb{Z}_q^*$ to $\mathbb{T}$.

   - $\chi(m)\chi(n) = \chi(mn)$
   - Set of all Dirichlet characters mod q forms a group.
   - There are $\phi(q)$ Dirichlet characters mod q.
   - $\chi(m)$ is $\phi(q)$-th root of unity.
   - Dirichlet character is trivial if $\chi \equiv 1$ (it's the identity in the group).
   - Dirichlet character, $\chi : \mathbb{Z}_q^* \to \mathbb{T}$, can be extended to $\chi : \mathbb{Z} \to \mathbb{T}$ be setting $\chi(n) = 0$ for $(n, q) \neq 1$ and $\chi(n) = \chi(n + q)$ for all q.
   - Orthogonality relation: $\frac{1}{\phi(q)} \sum_{\chi \bmod q} \chi(n)\overline{\chi(a)} = I(n \equiv a \bmod q)$

   (e) Generalized Chebyshev function

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

   - Assuming GRH, if χ is nontrivial, $\psi(x, \chi) \ll \sqrt{x} \log^2 x$. If χ_0 is trivial, then $\psi(x, \chi_0) = x + O(\sqrt{x} \log^2(qx))$

   (f) Möbius function

   Definition) For positive integer n, $\mu(n) = \begin{cases} (-1)^k & \text{if n is square-free with k distinct prime factors,} \\ 0 & \text{if n is not square-free} \end{cases}$

   - It's multiplicative.

   (g) Gauss sum and Ramanujan's sum

   Definition) $\tau(\chi) = \sum_{a \bmod q} \chi(a)e(a/q)$

   - $|\tau(\chi)| \leq \sqrt{q}$
   - $\tau(\chi_0) = \mu(q)$

2. **Outline of the proof**

We will show that

$$\sum_{n_1+n_2+n_3=N} \Lambda(n_1)\Lambda(n_2)\Lambda(n_3) \sim \frac{N^2}{2}\mathfrak{G}(N) \quad \cdots (1)$$

where $\mathfrak{G}(N) = \prod_{p|N}(1-\frac{1}{(p-1)^2})\prod_{p\nmid N}(1+\frac{1}{(p-1)^3})$. When N is odd, $\mathfrak{G}(N) \gg 1$, and since the number of prime squares and cubes, etc. is small, we can conclude that there are many ways of writing N as a sum of three primes.

To show (1), we write

$$\sum_{n_1+n_2+n_3=N} \Lambda(n_1)\Lambda(n_2)\Lambda(n_3) = \int_0^1 f(\alpha)^3 e(-N\alpha)d\alpha$$

where $f(\alpha) = \sum_{n\le N}\Lambda(n)e(n\alpha)$. We choose the major and minor arc and estimate the integral assuming Generalized Riemann Hypothesis.

3. **Proof of the theorem**

Lemma 1. Let a/q be a rational number with $(a,q)=1$. Then assuming GRH, we have

$$\sum_{n\le x}\Lambda(n)e(na/q) = \frac{\mu(q)}{\phi(q)}x + O(\sqrt{qx}\log^2 x)$$

Proof

Let $q = {p_1}^{q_1}{p_2}^{q_2}\cdots{p_k}^{q_k}$, where $p_1, p_2, \cdots, p_k$ are prime. If $(n,q)\neq 1$, then $\Lambda(n)e(na/q)$ is 0 if n is not a prime power. So,

$$\sum_{\substack{n\le x\\(n,q)\neq 1}}\Lambda(n)e(na/q) \ll \sum_{\substack{n\le x\\(n,q)\neq 1}}\Lambda(n) = \sum_{l=1}^{k}\sum_{a=1}^{\lfloor \log_{p_l} x\rfloor}\Lambda(p_l^a) \le \sum_{l=1}^{k}\log x \ll \sqrt{q}\log x$$

Now, note that

$$\begin{aligned} e(an/q) &= \sum_{b \bmod q} e(b/q)I(b=an) = \sum_{b \bmod q} e(b/q)\left(\frac{1}{\phi(q)}\sum_{\chi \bmod q}\chi(b)\overline{\chi(an)}\right) \\ &= \frac{1}{\phi(q)}\sum_{\chi \bmod q}\overline{\chi(an)}\left(\sum_{b \bmod q}\chi(b)e(b/q)\right) = \frac{1}{\phi(q)}\sum_{\chi \bmod q}\overline{\chi(an)}\tau(\chi) \end{aligned}$$

So,

$$\begin{aligned} \sum_{\substack{n\le x\\(n,q)=1}}\Lambda(n)e(an/q) &= \sum_{\substack{n\le x\\(n,q)=1}}\Lambda(n)\left(\frac{1}{\phi(q)}\sum_{\chi \bmod q}\overline{\chi(an)}\tau(\chi)\right) = \frac{1}{\phi(q)}\sum_{\chi \bmod q}\overline{\chi(a)}\tau(\chi)\left(\sum_{\substack{n\le x\\(n,q)=1}}\overline{\chi(n)}\Lambda(n)\right) \\ &= \frac{1}{\phi(q)}\sum_{\chi \bmod q}\overline{\chi(a)}\tau(\chi)\psi(x,\overline{\chi}) \quad \cdots (2) \end{aligned}$$

We know $|\overline{\chi(a)}| \leq 1$. By Gauss's sum, we know that $\tau(\chi) \leq \sqrt{q}$. When χ is nontrivial $\psi(x, \overline{\chi}) \ll \sqrt{x}\log^2 x$. For a trivial character, χ_0, we have $\overline{\chi_0(a)}\tau(\chi_0)\psi(x, \overline{\chi_0}) = \mu(q)(x + O(\sqrt{x}\log^2 x))$. So, (2) is equal to

$$O(\sqrt{qx}\log^2 x) + \frac{\mu(q)}{\phi(q)}(x + O(\sqrt{x}\log^2 x))$$

Therefore,

$$\begin{aligned}
\sum_{n\leq x} \Lambda(n)e(na/q) &= \sum_{\substack{n\leq x\\(n,q)\neq 1}} \Lambda(n)e(na/q) + \sum_{\substack{n\leq x\\(n,q)=1}} \Lambda(n)e(na/q) \\
&= O(\sqrt{q}\log x) + O(\sqrt{qx}\log^2 x) + \frac{\mu(q)}{\phi(q)}(x + O(\sqrt{x}\log^2 x)) \\
&= \frac{\mu(q)}{\phi(q)}x + O(\sqrt{qx}\log^2 x)
\end{aligned}$$

□

Lemma 2. Let $\alpha = a/q + \beta$ where $(a, q) = 1$. Then assuming GRH, we have

$$f(\alpha) = \frac{\mu(q)}{\phi(q)} \sum_{n\leq N} e(\beta n) + O((1 + |\beta|N)\sqrt{qN}\log^2 N)$$

Proof

$$\begin{aligned}
f(\alpha) &= \sum_{n\leq N} \Lambda(n)e(n\cdot\frac{a}{q})e(n\beta) = \sum_{n\leq N} e(n\beta)\left(\sum_{k\leq n}\Lambda(k)e(k\cdot\frac{a}{q}) - \sum_{k\leq n-1}\Lambda(k)e(k\cdot\frac{a}{q})\right) \\
&= \sum_{n\leq N} e(n\beta)\left(\frac{\mu(q)}{\phi(q)} + E(n, a/q) - E(n-1, a/q)\right) \qquad \left(E(n, a/q) \text{ is } \sum_{k\leq n}\Lambda(k)e(ka/q) - \frac{\mu(q)}{\phi(q)}n\right) \\
&= \frac{\mu(q)}{\phi(q)}\sum_{n\leq N} e(n\beta) + \sum_{n\leq N} e(n\beta)\left(E(n, a/q) - E(n-1, a/q)\right) \\
&= \frac{\mu(q)}{\phi(q)}\sum_{n\leq N} e(n\beta) + (e(N\beta)E(N, a/q) - e(1)E(0, a/q)) - \sum_{n\leq N-1} E(n, a/q)(e((n+1)\beta) - e(n\beta)) \\
&= \frac{\mu(q)}{\phi(q)}\sum_{n\leq N} e(n\beta) + O(\sqrt{qN}\log^2 N) + O(N)\cdot O(\sqrt{qN}\log^2 N)\cdot O(|\beta|)
\end{aligned}$$

and we are done. □

Corollary 3. Select $Q = N^{\frac{2}{3}}$, and let $|\alpha - a/q| \leq 1/(qQ)$ with $(a, q) = 1$ and $q \leq Q$. Then assuming GRH,

$$f(\alpha) \ll \frac{N}{\phi(q)} + N^{\frac{5}{6}+\epsilon}$$

Proof

From lemma 2, we have

$$f(\alpha) \ll \frac{N}{\phi(q)} + (1 + \frac{N}{qQ})\sqrt{qN}\log^2 N \ll \frac{N}{\phi(q)} + (\sqrt{QN} + \frac{N^{\frac{3}{2}}}{Q})\log^2 N$$

and set $Q = N^{\frac{2}{3}}$ and the result follows. □

Now, we choose the major and minor arc. Take $Q = N^{\frac{2}{3}}$. By Dirichlet, we have $|\alpha - a/q| < 1/(qQ)$ for some $q \leq Q$. Let α be on the major arc if $q \leq (\log N)^{10}$.

Minor arc contribution

$$\int_{\mathfrak{m}} f(\alpha)^3 e(-N\alpha) d\alpha \ll \frac{N^2}{\log^8 N}$$

Proof

We know that $\phi(q) \gg q/\log q$ and $N > N^{\frac{2}{3}} = Q > q > (\log N)^{10}$ for α on the minor arc. So, $\phi(q) \gg (\log N)^9$. Therefore, $f(\alpha) \ll \frac{N}{(\log N)^8}$ by corollary 3.

$$\begin{aligned}
\int_{\mathfrak{m}} f(\alpha)^3 e(-N\alpha) d\alpha &\ll \int_{\mathfrak{m}} f(\alpha)^3 d\alpha \ll \frac{N}{(\log N)^9} \int_{\mathfrak{m}} f(\alpha)^2 d\alpha \ll \frac{N}{(\log N)^9} \int_0^1 |f(\alpha)|^2 d\alpha = \frac{N}{(\log N)^9} \int_0^1 f(\alpha) f(-\alpha) d\alpha \\
&= \frac{N}{(\log N)^9} \sum_{\substack{n \leq N \\ m \leq N \\ n-m=0}} \Lambda(n)\Lambda(m) = \frac{N}{(\log N)^9} \sum_{n \leq N} \Lambda(n)^2 \ll \frac{N^2}{(\log N)^8}
\end{aligned}$$

□

Major arc contribution

$$\int_{\mathfrak{M}} f(\alpha)^3 e(-N\alpha) d\alpha \sim \frac{N^2}{2} \mathfrak{G}(N)$$

Proof

Note that for each rational number a/q, the interval of α, $|\alpha - a/q| < 1/(qQ)$, are disjoint. So, we have

$$\int_{\mathfrak{M}} f(\alpha)^3 e(-N\alpha) d\alpha = \sum_{q \leq (\log N)^{10}} \sum_{\substack{1 \leq a \leq q \\ (a,q)=1}} \int_{-1/(qQ)}^{1/(qQ)} f(a/q + \beta)^3 e(-N(a/q + \beta)) d\beta$$

From lemma 2,

$$\begin{aligned}
f(a/q + \beta)^3 &= (\frac{\mu(q)}{\phi(q)} \sum_{n \leq N} e(\beta n))^3 + (\frac{\mu(q)}{\phi(q)} \sum_{n \leq N} e(\beta n))^2 O((1 + |\beta|N)\sqrt{qN} \log^2 N) \\
&\quad + (\frac{\mu(q)}{\phi(q)} \sum_{n \leq N} e(\beta n)) O((1 + |\beta|N)\sqrt{qN} \log^2 N)^2 + O((1 + |\beta|N)\sqrt{qN} \log^2 N)^3
\end{aligned}$$

Let's consider two cases. If $|\beta| \gg N^{-\frac{9}{10}}$, then $\sum_{n \leq N} e(\beta n) \ll 1/\|\beta\| \ll N^{\frac{9}{10}}$ and $O((1 + |\beta|N)\sqrt{qN} \log^2 N) \ll N^{\frac{5}{6}+\epsilon}$ since $|\beta| < 1/(qQ) < 1/Q = N^{-\frac{2}{3}}$. If $|\beta| \ll N^{-\frac{9}{10}}$, then $\sum_{n \leq N} e(\beta n) \ll N$ and $O((1 + |\beta|N)\sqrt{qN} \log^2 N) \ll N^{\frac{3}{5}+\epsilon}$. In both cases, we get $f(a/q + \beta)^3 = (\frac{\mu(q)}{\phi(q)} \sum_{n \leq N} e(\beta n))^3 + O(N^{\frac{79}{30}+\epsilon})$.

Therefore, the major arc contribution is

$$\int_{\mathfrak{M}} f(\alpha)^3 e(-N\alpha)d\alpha = \sum_{q\leq(\log N)^{10}} \sum_{\substack{1\leq a\leq q\\(a,q)=1}} \int_{-1/(qQ)}^{1/(qQ)} \left(\left(\frac{\mu(q)}{\phi(q)}\sum_{n\leq N} e(\beta n)\right)^3 + O(N^{\frac{79}{30}+\epsilon})\right) e(-N(a/q+\beta))d\beta$$

$$= \sum_{q\leq(\log N)^{10}} \frac{\mu(q)^3}{\phi(q)^3}\left(\sum_{\substack{1\leq a\leq q\\(a,q)=1}} e(-N(a/q))\right)\left(\int_{-1/(qQ)}^{1/(qQ)}\left(\sum_{n\leq N} e(\beta n)\right)^3 e(-N\beta)d\beta\right) + O(N^{\frac{59}{30}+\epsilon}) \quad \cdots (3)$$

Since $\sum_{n\leq N} e(\beta n) \ll 1/\|\beta\|$, so

$$\int_{1/qQ}^{1-1/qQ}\left(\sum_{n\leq N} e(\beta n)\right)^3 e(-N\beta)d\beta \ll \int_{1/qQ}^{1-1/qQ}\frac{1}{\|\beta\|^3}d\beta = 2\int_{1/qQ}^{1/2}\frac{1}{\beta^3}d\beta = 2(\frac{1}{2(1/qQ)^2} - \frac{1}{2\cdot 1/2}) \ll q^2Q^2$$

We also have

$$\int_0^1\left(\sum_{n\leq N} e(\beta n)\right)^3 e(-N\beta)d\beta = \int_0^1 \sum_{n_1,n_2,n_3\leq N} e((n_1+n_2+n_3-N)\beta) = (\#\text{ of } n_1+n_2+n_3=N) = \binom{N-1}{2}$$

Therefore,

$$\int_{-1/(qQ)}^{1/(qQ)}\left(\sum_{n\leq N} e(\beta n)\right)^3 e(-N\beta)d\beta = \int_0^1 - \int_{1/qQ}^{1-1/qQ} \sim \frac{N^2}{2} + O(q^2Q^2)$$

Using this in (3) yields

$$\sim \frac{N^2}{2}\sum_{q\leq(\log N)^{10}}\frac{\mu(q)^3}{\phi(q)^3}\left(\sum_{\substack{1\leq a\leq q\\(a,q)=1}} e(-N(a/q))\right) + O(N^{\frac{59}{30}+\epsilon})$$

We know that the sum inside is at most $\phi(q)$. $\sum_{q>(\log N)^{10}}\frac{\mu(q)^3}{\phi(q)^3}\left(\sum_{(a,q)=1} e(-N(a/q))\right) \leq \sum_{q>(\log N)^{10}}\frac{\mu(q)^3}{\phi(q)^2} \leq \sum_{q>(\log N)^{10}}\frac{1}{\phi(q)^2}$. So, by extending the sum to infinity, we get

$$\sim \frac{N^2}{2}\sum_{q=1}^{\infty}\frac{\mu(q)^3}{\phi(q)^3}\left(\sum_{\substack{1\leq a\leq q\\(a,q)=1}} e(-N(a/q))\right)$$

$\mu(q)$, $\phi(q)$ and $\sum_{\substack{1\leq a\leq q\\(a,q)=1}} e(-N(a/q))$ are all multiplicative, so

$$\frac{N^2}{2}\prod_p\left(1+\frac{\mu(p)^3}{\phi(p)^3}\sum_{\substack{1\leq a\leq p\\(a,p)=1}} e(-N(a/p))\right) = \frac{N^2}{2}\prod_p\left(1-\frac{1}{(p-1)^3}(p\cdot I(p|N)-1)\right) = \frac{N^2}{2}\prod_{p|N}(1-\frac{1}{(p-1)^2})\prod_{p\nmid N}(1+\frac{1}{(p-1)^3})$$

and we are done. $\square$

So we finally have

$$\sum_{n_1+n_2+n_3=N} \Lambda(n_1)\Lambda(n_2)\Lambda(n_3) \sim \frac{N^2}{2}\mathfrak{G}(N)$$

When N is odd, we have

$$\mathfrak{G}(N) = \prod_{p|N}(1-\frac{1}{(p-1)^2})\prod_{p\nmid N}(1+\frac{1}{(p-1)^3}) \geq (1-\frac{1}{2^2}-\frac{1}{4^2}-\frac{1}{6^2}-\cdots)\cdot(1+\frac{1}{1}) = 2(1-\frac{1}{4}\cdot\frac{\pi^2}{6})$$

so $\sum_{n_1+n_2+n_3=N} \Lambda(n_1)\Lambda(n_2)\Lambda(n_3) \gg N^2$