قضیه‌ی وینوگرادوف

میلاد برزگر

با توجه به پیشرفت‌های اخیر در نظریه‌ی تحلیلی اعداد، بر آن شدیم مقاله‌ای در این شاخه در مجله داشته باشیم.

۱ مقدمه

گلدباخ در سال ۱۷۴۲ در نامه‌ای به لئونارد اویلر حدس زیر را مطرح کرد:

> هر عدد صحیح بزرگ‌تر از ۵ را می‌توان به صورت مجموع سه عدد اول نوشت.

اویلر در پاسخ صورت معادلی از این مسئله را مطرح که امروزه با نام «حدس قوی گلدباخ» شناخته می‌شود:

> هر عدد زوج بزرگ‌تر از ۲ را می‌توان به صورت مجموع دو عدد اول نوشت.

توجه کنید که اگر $2n+2$ را بتوان به صورت مجموع سه عدد اول نوشت، یکی از آن‌ها باید زوج و در نتیجه برابر ۲ باشد. با حذف ۲ از طرفین نتیجه می‌شود $2n$ را می‌توان به صورت مجموع دو عدد اول نوشت. همچنین اگر $2n=p+q$، که p و q اعداد اول هستند، آن‌گاه می‌توان نوشت $2n+3=p+q+3$ و $2n+2=p+q+2$. بنابراین دو مسئله‌ی مطرح شده در بالا با هم معادل هستند. حدس قوی گلدباخ تاکنون حل نشده است. اما درستی آن به کمک الگوریتم های کامپیوتری برای $n \leq 1/605 \times 10^{18}$ بررسی شده است. همچنین پیشرفت زیادی در راه‌حل این مسئله حاصل نشده است.

اگر $2n=p+q$ باشد که p و q اعداد اول هستند، p و q باید هر دو فرد باشند (چون در غیر این صورت n باید مساوی ۲ باشد). بنابراین $2n+3=p+q+3$. این نتیجه می‌دهد اگر حدس قوی گلدباخ درست باشد، آن‌گاه

> هر عدد فرد بزرگ‌تر از ۷ را می‌توان به صورت مجموع سه عدد اول فرد نوشت.

مسأله فوق «حدس ضعیف گلدباخ» نامیده می‌شود. این مسئله نیز حل نشده است، اما برخلاف صورت قوی حدس گلدباخ پیشرفت‌های زیادی در جهت اثبات آن حاصل شده و ما هم‌اکنون به اثبات آن نزدیک هستیم.

هاردی و لیتلوود در سال ۱۹۲۳، با فرض درستی حدس قوی ریمان (همه‌ی صفرهای غیربدیهی تابع L دیریکله روی خط $Re(z)=\frac{1}{2}$ قرار دارند)، و با به کارگیری Circle method (که در این مقاله این روش را توضیح می‌دهیم) ثابت کردند حدس ضعیف گلدباخ برای اعداد صحیح «به اندازه کافی بزرگ» درست است. لیتلوود نشان داد «به اندازه کافی بزرگ» یعنی برای اعداد بیش‌تر از 10^{50}. وینوگرادوف[۱] در سال ۱۹۳۷ با ایجاد تغییراتی در روش هاردی و لیتلوود و به کارگیری حکمی از نظریه اعداد در مورد اعداد اول (Siegel–Walfisz theorem) موفق شد بدون استفاده از فرضیه‌ی ریمان، حدس ضعیف گلدباخ را برای اعداد «به اندازه کافی بزرگ» ثابت کند. وینوگرادوف در مقاله‌ی خود معنی «به اندازه کافی بزرگ» را مشخص نکرد، اما بیان داشت که می‌توان روش او را دقیق‌تر کرد و کران موردنظر را مشخص کرد. در سال ۱۹۳۹ شاگرد وینوگرادوف به نام بوروزدین[۲] با دقیق‌سازی روش وینوگرادوف کران $10^{7\times 10^{6}} \approx 3^{3^{15}}$ را به دست آورد. امروزه این کران تا $e^{3100} \approx 2\times 10^{1346}$ کاهش یافته است. اما این عدد برای بررسی‌های کامپیوتری بسیار بزرگ است (کامپیوترها موفق به چک کردن حدس تا 10^{18} شده‌اند) و بنابراین این صورت از حدس ریمان نیز حل نشده باقی مانده است.

هدف ما در این‌جا اثبات «قضیه‌ی وینوگرادوف» است. روشی که ارائه می‌دهیم، روش خود وینوگرادوف برای اثبات این قضیه است. فرض کنید $\mathbb{P}$ مجموعه‌ی اعداد طبیعی اول باشد. تابع شمارنده‌ی تعداد روش‌های نوشتن عدد صحیح N به صورت مجموع سه عدد اول این‌گونه تعریف می‌شود.

$$r(N)=\sum_{\substack{p_1+p_2+p_3=N\\ p_1,p_2,p_3\in\mathbb{P}}} 1$$

قضیه‌ی وینوگرادوف یک فرمول مجانبی برای $r(N)$ بدست می‌دهد که به راحتی از آن نتیجه می‌شود برای Nهای فرد به اندازه کافی بزرگ $r(N)>0$ و به این ترتیب حدس ضعیف گلدباخ برای اعداد به اندازه کافی بزرگ اثبات می‌شود.

قضیه ۱. (*قضیه‌ی وینوگرادوف*): *تابع حسابی $G(N)$ و اعداد مثبت c_1 و c_2 موجودند به طوری که*

i) *برای هر N فرد:* $c_1 < G(N) < c_2$

[۱] Ivan Matveevich Vinogradov
[۲] Borozdin

(*ii* *برای N فرد به اندازه کافی بزرگ:*

$$r(N) = G(N)\frac{N^{2}}{2(\log N)^{3}}\Big(1+O\big(\frac{\log\log N}{\log N}\big)\Big)$$

که $G(N)$ سری تکین ($singular\ series$) برای حدس ضعیف گلدباخ نامیده می‌شود.

اگر قضیه‌ی فوق اثبات شود، از (i) نتیجه می‌شود $G(N)$ صفر نیست و کران‌دار است. همچنین بقیه‌ی جملات در سمت راست تساوی (ii) وقتی N بزرگ است، مثبت بوده و در نتیجه $r(N) > 0$.

۲ سری تکین ($G(N)$)

این تابع به طور طبیعی در محاسبات ما ظاهر خواهد شد. اما برای راحتی آن را در این‌جا معرفی می‌کنیم و خواص آن را مورد برررسی قرار می‌دهیم. فرض کنید $q \in \mathbb{N}$ و $N \in \mathbb{Z}$، جمع رامانوجان [3] به صورت زیر تعریف می‌شود

$$C_q(N) = \sum_{\substack{a=1\\(a,q)=1}}^{q} e\Big(\frac{aN}{q}\Big)$$

که در آن $e(x) = e^{2\pi ix}$ است.

با توجه به تعریف فوق سری تکین این‌گونه محاسبه می‌شود

$$G(N) = \sum_{q=1}^{\infty}\frac{\mu(q)C_q(N)}{\phi(q)^{3}}$$

لم ۲. *فرض کنید f یک تابع ضربی [4] باشد. اگر*

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

که p^k بین تمام توان‌های اعداد اول تغییر می‌کند. در این صورت

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

.

اثبات. از فرض نتیجه می‌شود متناهی توان عدد اول p^k موجود است که $|f(p^k)| \geq 1$. قرار می‌دهیم:

$$A = \prod_{|f(p^k)|\geq 1} |f(p^k)| \quad \Rightarrow A \geq 1$$

فرض کنید $0 < \epsilon < A$. در این صورت متناهی عدد اول p^k موجود است که $|f(p^k)| \geq \epsilon/A$. بنابراین متناهی عدد صحیح n موجود است که به ازای هر p^k که $p^k|n$ و $p \in \mathbb{P}$ داشته باشیم

$$|f(p^k)| \geq \epsilon/A$$

در نتیجه اگر n به اندازه‌ی کافی بزرگ باشد، $p \in \mathbb{P}$ و $k \in \mathbb{N}$ موجود است که $|f(p^k)| < \epsilon/A$. در نتیجه می‌توان نوشت

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

که $p_1, \ldots, p_{r+s+t}$ اعداد اول متمایزاند و داریم

$$\begin{aligned}
&1 \leq |f(p_i^{k_i})| &&;\ i = 1, 2, \ldots, r\\
&\epsilon/A \leq |f(p_i^{k_i})| < 1 &&;\ i = r+1, r+2, \ldots, r+s\\
&|f(p_i^{k_i})| < \epsilon/A &&;\ i = r+s+1, \ldots, r+s+t
\end{aligned}$$

و $t \geq 1$ می‌باشد. در نتیجه

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

این اثبات را کامل می‌کند. □

قضیه ۳. *$G(N)$ به طور مطلق و یکنواخت همگرا است و ضرب اویلری آن به صورت زیر است*

$$G(N) = \prod_{p}\Big(1+\frac{1}{(p-1)^{3}}\Big).\prod_{p/N}\Big(1+\frac{1}{p^{2}-3p+3}\Big); p \in \mathbb{P}$$

همچنین اعداد مثبت c_1 و c_2 موجودند که برای Nهای فرد $c_1 < G(N) < c_2$ باشد. و برای هر $\epsilon > 0$ داریم

$$G(N,Q) := \sum_{q\leq Q}\frac{\mu(q)C_q(N)}{\phi(q)^{3}} = G(N) + O(Q^{-(1-\epsilon)})$$

که ثابت موردنیاز (برای O) فقط به ϵ وابسته است.

اثبات. برای هر عدد اول p داریم $\frac{p}{p-1} \leq 2$. در نتیجه داریم

$$\begin{aligned}
\frac{p^{m(1-\epsilon)}}{\phi(p^m)} &= \frac{p^{m(1-\epsilon)}}{p^{m-1}(p-1)}\\
&= \frac{p}{p-1}.\frac{p^{m(1-\epsilon)}}{p^m} \leq \frac{2}{p^{m\epsilon}}\\
\Rightarrow \lim_{p^m\to\infty}&\frac{p^{m(1-\epsilon)}}{\phi(p^m)} = 0
\end{aligned}$$

قرار می‌دهیم $f(n) = \frac{n^{(1-\epsilon)}}{\phi(n)}$. مشخص است که f ضربی است. در نتیجه طبق لم ۱ داریم

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

این نتیجه می‌دهد برای qهای به اندازه کافی بزرگ $\phi(q) \geq q^{1-\epsilon}$. داریم

$$\Big|\frac{\mu(q)C_q(N)}{\phi(q)^{3}}\Big| = \frac{|C_q(N)|}{\phi(q)^{3}} \leq \frac{\phi(q)}{\phi(q)^{3}} = \frac{1}{\phi(q)^{2}} \ll \frac{1}{q^{2-\epsilon}}$$

[3] Ramanujan's sum

[4] $(a,b) = 1 \Rightarrow f(ab) = f(a)f(b)$

در نتیجه $G(N)$ به طور مطلق و یکنواخت همگرا است. همچنین نتیجه می‌شود

$$G(N)-G(N,Q) \ll \sum_{q>Q}\frac{1}{\phi(q)^2} \ll \sum_{q>Q}\frac{1}{q^{2-\epsilon}} \ll \frac{1}{Q^{1-\epsilon}}$$
$$\Rightarrow G(N,Q)=G(N)+O(Q^{-(1-\epsilon)})$$

$C_q(N)$ یک تابع ضربی از q است. برای اثبات این مطلب فرض کنید q و q' دو عدد نسبت به هم اول باشند. در این صورت هر کلاس از اعداد نسبت به qq' اول را می‌توان به صورت یکتا به شکل $aq'+a'q$ نوشت که $1<a<q$ و $1<a'<q'$ و $(a,q)=(a',q')=1$. با توجه به این نکته، داریم

$$\begin{aligned}
c_q(N)c_{q'}(N) &= \sum_{\substack{a=1\\(a,q)=1}}^{q} e(aN/q).\sum_{\substack{a'=1\\(a',q')=1}}^{q'} e(a'N/q') \\
&= \sum_{\substack{a=1\\(a,q)=1}}^{q}\sum_{\substack{a'=1\\(a',q')=1}}^{q'} e\Big(\frac{(aq'+a'q)}{qq'}N\Big) \\
&= \sum_{\substack{a''=1\\(a'',qq')=1}}^{qq'} e(a''N/qq') = c_{qq'}(N) \\
&\Rightarrow c_q(N)c_{q'}(N)=c_{qq'}(N)
\end{aligned}$$

که نتیجه می‌دهد $\frac{\mu(q)c_q(N)}{\phi(q)^2}$ نسبت به q ضربی است.

همچنین اگر p اول باشد $c_p(N)=\begin{cases} p-1 & p|N \\ -1 & p\nmid N\end{cases}$ و برای $i\geq 2$ داریم $\mu(p^i)=0$. در نتیجه داریم

$$\begin{aligned}
G(N) &= \prod\Big(1+\sum_{i=1}^{\infty}\frac{\mu(p^i)c_{p^i}(N)}{\phi(p^i)^2}\Big)=\prod_p\Big(1-\frac{c_p(N)}{\phi(p)^2}\Big) \\
&= \prod_{p\nmid N}\Big(1+\frac{1}{(p-1)^2}\Big).\prod_{p|N}\Big(1-\frac{1}{(p-1)^2}\Big) \\
&= \prod_p\Big(1+\frac{1}{(p-1)^2}\Big).\prod_{p|N}\Big(1-\frac{1}{p^2-3p+3}\Big)
\end{aligned}$$

داریم:

$$\begin{aligned}
1 &\leq \prod_p\Big(1+\frac{1}{(p-1)^2}\Big) \\
&\leq \prod_p\Big(1+\frac{1}{p-1}\Big)=\prod_p\frac{p}{p-1}=\zeta(2) \\
\frac{1}{2\zeta(2)} &= \prod_{p\neq 2}\Big(1-\frac{1}{p}\Big)\leq\prod_p\Big(1-\frac{1}{p-1}\Big) \\
&\leq \prod_p\Big(1-\frac{1}{p-1}\Big)\Big(1+\frac{1}{p-1}\Big) \\
&= \prod_p\Big(1-\frac{1}{(p-1)^2}\Big)\leq 1
\end{aligned}$$

این وجود c_2 و c_1 را نتیجه می‌هد. □

۳ Circle Method

منشأ این روش مقاله‌ای از هاردی و رامانوجان است که در سال ۱۹۱۸ منتشر شد و در مورد تعداد روش‌های نوشتن یک عدد طبیعی به صورت مجموعی از اعداد طبیعی بحث می‌کرد. در سال ۱۹۲۰ هاردی و لیتلوود در مجموعه‌ای از مقالات با عنوان Some problems of 'partitio numerorum' روش Circle method را به طور جدی معرفی کردند و آن را برای بررسی مسائل گوناگون به کار بستند. مقالات شماره III و V از این سری به بررسی حدس گلدباخ پرداخته است. ما در این‌جا به طور خلاصه این روش را معرفی می‌کنیم

فرض کنید A مجموعه‌ای دلخواه از اعداد طبیعی باشد. تابع مولد A به این صورت است

$$f(z)=\sum_{a\in A}z^a$$

و فرض می‌کنیم $|z|<1$ تا همگرایی برآورده شود و قرار می‌دهیم

$$r_{A,S}(N)=\#\{(a_1,\dots,a_s)\in A^s | a_1+\cdots+a_s=N\}$$

در این صورت داریم $f(z)^s=\sum_{N=0}^{\infty}r_{A,S}(N)z^N$ و با کمک قضیه کوشی می‌توان $r_{A,S}(N)$ را این‌گونه محاسبه کرد

$$r_{A,S}(N)=\frac{1}{2\pi i}\int_{|z|=\rho}\frac{f(z)^s}{z^{N+1}}\,\mathrm{d}z \quad ;\rho\in(0,1)$$

این شکل اصلی circle method است که توسط هاردی و لیتلوود ارائه شد. اما قسمت سخت کار تقریب زدن انتگرال فوق است که هاردی و لیتلوود برای این کار، دامنه انتگرال ($|z|=\rho$) را به دو زیرمجموعه‌ی «کمان‌های بزرگ» (major arcs) و «کمان‌های کوچک» (minor arcs) تقسیم کردند (طوری که بتوان تقریب‌های

مناسب را اعمال کرد) و محاسبات لازم را انجام دادند. اما همان طور که در مقدمه اشاره شد این روش برای حل «قضیه سه اول» (هر عدد فرد بزرگ را می‌توان به صورت مجموع سه عدد اول نوشت) کارساز نبود. کاری که وینوگرادوف برای سادگی کار انجام داد از قرار زیر است:

فرض کنید بخواهیم $r_{A,S}(N)$ را مورد بررسی قرار دهیم. توابع زیر را در نظر می‌گیریم

$$F(\alpha)=\sum_{\substack{a\in A\\ a\le N}} e(a\alpha) \Rightarrow F(\alpha)^s = \sum_{m=0}^{sN} r^{(N)}_{A,S}(m)\, e(m\alpha)$$

که $r^{(N)}_{A,S}(m)$ تعداد روش‌های نوشتن m به صورت مجموعی از اعضای کمتر از N مجموعه‌ی A است. در این صورت به وضوح داریم $r^{(N)}_{A,S}(N)=r_{A,S}(N)$. همچنین داریم

$$\int_0^1 e(m\alpha)e(-n\alpha) = \begin{cases}1 & m=n\\ 0 & m\neq n\end{cases}$$

در نتیجه می‌توان $r_{A,S}(N)$ را این‌گونه محاسبه کرد

$$r_{A,S}(N)=\int_0^1 F(\alpha)^s e(-n\alpha)\,\mathrm{d}\alpha$$

ایده‌ی دیگر که در محاسبات وینوگرادوف وجود دارد، این است که او به جای $r(N)$، روش فوق را برای تقریب زدن تابع $R(N)=\sum_{p_1+p_2+p_3=N}\log p_1\log p_2\log p_3$ به کار می‌گیرد و از این تقریب، به راحتی قضیه‌ی ۱ در مورد $r(N)$ نتیجه می‌شود. در واقع داریم:

$$F(\alpha)=\sum_{p\le N}\log p . e(p\alpha) \Rightarrow R(N)=\int_0^1 F(\alpha)^3 e(-N\alpha)\,\mathrm{d}\alpha \qquad (1)$$

۴ تجزیه به major arcs و minor arcs

همان‌گونه که در بالا اشاره شد، بازه‌ی $[0,1]$ را به دو مجموعه‌ی M (کمان‌های بزرگ) و m (کمان‌های کوچک) افراز می کنیم. یک $B>0$ در نظر می‌گیریم و قرار می‌دهیم $Q=(\log N)^B$. برای $1\le q\le Q$ و $0\le a\le q$ که $(a,q)=1$ تعریف می‌کنیم

$$M(q,a)=\{\alpha\in[0,1] : |\alpha-\frac{a}{q}|\le Q/N\}$$

اگر $a/q\neq a'/q'$ باشد، آن‌گاه $|aq'-a'q|\ge 1$ و در نتیجه داریم

$$\begin{aligned}\alpha\in M(q,a)\cap M(q',a') \Rightarrow \frac{1}{Q^2} &\le \frac{1}{qq'}\\ &\le \frac{|aq'-a'q|}{qq} = \Big|\frac{a}{q}-\frac{a'}{q'}\Big|\\ &\le \Big|\frac{a}{q}-\alpha\Big| + \Big|\alpha-\frac{a'}{q'}\Big|\\ &\le \frac{2Q}{N}\\ \Rightarrow N\le 2Q^3 &= 2(\log N)^{3B}\end{aligned}$$

که برای Nهای بزرگ برقرار نیست. بنابراین وقتی N به اندازه کافی بزرگ است، $M(q,a)$ها دو به دو متمایز هستند. مجموعه‌ی M را این‌گونه تعریف می‌کنیم

$$M:=\bigcup_{q=1}^{Q}\bigcup_{\substack{Q=0\\(Q,q)=1}}^{q} M(q,a)\subseteq[0,1]$$

و همچنین $m:=[0,1]\backslash M$.

در نتیجه می‌توانیم رابطه‌ی ۱ را به این صورت بنویسیم

$$R(N)=\int_M F(\alpha)^3e(-N\alpha)\,\mathrm{d}\alpha+\int_m F(\alpha)^3e(-N\alpha)\,\mathrm{d}\alpha$$

در ادامه به محاسبه‌ی دو انتگرال فوق می‌پردازیم.

۵ محاسبه‌ی انتگرال روی M

لم ۴. *فرض کنید* $u(\beta)=\sum_{m=1}^N e(m\beta)$. *در این صورت داریم*

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

اثبات. طبق آن‌چه در بخش ۳ گفتیم، تعداد راه‌های نوشتن N به صورت مجموع سه عدد طبیعی برابر است با $J(N)$ (که در صورت لم تعریف شده است). از طرفی از ترکیبیات می‌دانیم تعداد راه‌های نوشتن N به صورت مجموع سه عدد طبیعی برابر است با $\binom{N-1}{2}$. در نتیجه

$$J(N)=\binom{N-1}{2}=\frac{N^2}{2}+O(N)$$

اثبات لم به پایان رسید. □

لم ۵. $c_q(n)=\sum_{d|(q,n)}\mu(q/d)d$. *این نتیجه می‌دهد که اگر* $(q,n)=1$ *آنگاه* $c_q(n)=\mu(q)$

اثبات. ابتدا توجه کنید که داریم

$$f_d(n):=\sum_{l=1}^{d} e(\frac{ln}{d})=\begin{cases}d & d|n\\ 0 & d\nmid n\end{cases}$$

در نتیجه

$$\begin{aligned} c_q(n) &= \sum_{\substack{k=۱\\(k,q)=۱}}^{q} e\Big(\frac{kn}{q}\Big) = \sum_{k=۱}^{q} e\Big(\frac{kn}{q}\Big) \sum_{d|(k,q)} \mu(d) \\ &= \sum_{d|q}\mu(d)\sum_{\substack{k=۱\\d|k}}^{q} e\Big(\frac{kn}{q}\Big) \\ &= \sum_{d|q}\mu(d)\sum_{l=۱}^{q/d} e\Big(\frac{ln}{q/d}\Big) \\ &= \sum_{d|q}\mu(d) f_{q/d}(n) = \sum_{d|q}\mu(q/d) f_d(n) \\ &= \sum_{\substack{d|q\\d|n}}\mu(q/d)d = \sum_{d|(n,q)}\mu(q/d)d \end{aligned}$$

□

لم ۶. *برای هر $\alpha \in \mathbb{R}$ و $N_۱, N_۲ \in \mathbb{Z}$ با شرط $N_۱ < N_۲$، داریم*

$$\sum_{n=N_۱+۱}^{N_۲} e(\alpha n) \ll \min(N_۲ - N_۱, \|\alpha\|^{-۱})$$

که $\|\alpha\|$ یعنی فاصله‌ی α از نزدیک‌ترین عدد صحیح به آن.

اثبات.

$$\forall n \in \mathbb{Z} : |e(n\alpha)| = ۱ \Rightarrow \Big|\sum_{n=N_۱+۱}^{N_۲} e(\alpha N)\Big| \le \sum_{n=N_۱+۱}^{N_۲} ۱ = N_۲ - N_۱$$

اگر α صحیح باشد حکم واضح است. اگر α صحیح نباشد، آن‌گاه $\|\alpha\| > ۰$ و $e(n\alpha) \neq ۱$. با توجه به نکات داریم

$$\begin{aligned} \Big|\sum_{n=N_۱+۱}^{N_۲} e(\alpha n)\Big| &= \Big|e(\alpha(N_۱+۱)) \sum_{n=۰}^{N_۲-N_۱-۱} e(\alpha)^n\Big| \\ &= \Big|\frac{e(\alpha(N_۲-N_۱))-۱}{e(\alpha)-۱}\Big| \le \frac{۲}{|e(\alpha)-۱|} \\ &= \frac{۲}{|e(\alpha/۲)-e(-\alpha/۲)|} = \frac{۲}{|۲i\sin\pi\alpha|} \\ &= \frac{۱}{|\sin\pi\alpha|} = \frac{۱}{\sin\pi\|\alpha\|} \le \frac{۱}{۲\|\alpha\|} \end{aligned}$$

در نابرابری آخر از این استفاده کردیم که

$$۰ < \alpha < \frac{۱}{۲} \Rightarrow ۲\alpha < \sin\pi\alpha < \pi\alpha$$

(این حکم به راحتی از مشتق‌گیری به دست می‌آید و ما از آوردن اثبات خودداری می‌کنیم). این اثبات حکم را کامل می‌کند. □

در اثبات لم بعدی از قضیه‌ی Siegel–Walfisz در مورد چگالی اعداد اول در یک تصاعد حسابی استفاده خواهیم کرد. اثبات این قضیه را در این‌جا ارائه نمی دهیم. اثباتی از این قضیه در کتاب Davenport ارائه شده است

قضیه ۷. *(Siegel–Walfisz): اگر $q \ge ۱$ و $(a,q) = ۱$، آن‌گاه برای هر $C > ۰$، رابطه‌ی زیر برای $x \ge ۲$ برقرار است.*

$$\theta(x,q,a) := \sum_{\substack{p\le x\\p\equiv a(\mathrm{mod}\ q)}} \log p = \frac{z}{\phi(q)} + O\Big(\frac{x}{(\log x)^C}\Big)$$

که ثابت موردنیاز (برای O) فقط به C وابسته است.

لم ۸. *تعریف می‌کنیم $F_x(\alpha) := \sum_{p\le x}\log p.e(p\alpha)$. همچنین $C > ۰$. در این صورت برای $۱ \le q \le Q$ و $۱ \le a \le q$ که $(q,a) = ۱$ و $۱ \le x \le N$ داریم*

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

که ثابت موردنیاز فقط به B و C بستگی دارد (توجه کنید که قبلا تعریف کرده‌ایم $Q = (\log N)^B$)

اثبات. ابتدا توجه کنید که برای p اول، اگر $p \equiv r(\mathrm{mod}\ q)$ آن‌گاه $(r,q) \neq ۱ \iff p|q$. همچنین داریم

$$\begin{aligned} \sum_{\substack{r=۱\\(r,q)\neq ۱}}^{q} \sum_{\substack{p\le x\\p\equiv r\ (q)}} \log p.e(pa/q) &= \sum_{\substack{p\le x\\p|q}} \log p.e(pa/q) \\ &\ll \sum_{p|q}\log p \le \log q \end{aligned}$$

از نکات بالا نتیجه می‌شود

$$\begin{aligned}
F_x(a/q) &= \sum_{r=1}^{q} \sum_{\substack{p\le x\\ p\equiv r\ (q)}} \log p . e(pa/q) \\
&= \sum_{\substack{r=1\\ (r,q)=1}}^{q} \sum_{\substack{p\le x\\ p\equiv r\ (q)}} \log p . e(pa/q) + O(\log q) \\
&= \sum_{\substack{r=1\\ (r,q)=1}}^{q} e(ra/q) \sum_{\substack{p\le x\\ p\equiv r\ (q)}} \log p + O(\log Q) \\
&= \sum_{\substack{r=1\\ (r,q)=1}}^{q} e(ra/q)\theta(x,q,r) + O(\log Q) \\
&= \sum_{\substack{r=1\\ (r,q)=1}}^{q} e(ra/q)\Big(\frac{x}{\phi(q)} + O\big(\frac{x}{(\log x)^C}\big)\Big) + O(\log Q) \\
&= \frac{c_q(a)}{\phi(q)}x + O\big(\frac{qx}{(\log x)^C}\big) + O(\log Q) \\
&= \frac{\mu(q)}{\phi(q)}x + O\big(\frac{QN}{(\log N)^C}\big)
\end{aligned}$$

در تساوی آخر از لم ۵ استفاده کردیم. □

لم ۹. *فرض کنید $B,C>0$ و $C>2B$. اگر $\alpha\in M(q,a)$ و $\beta=\alpha-a/q$ آن‌گاه*

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

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

که ثابت‌های مورد نیاز فقط به B و C وابسته‌اند(باز هم فرض کردیم $Q=(\log N)^B$).

اثبات. طبق تعریف $M(q,a)$ داریم $|\beta|\le Q/N$. تعریف می‌کنیم

$$\lambda(m)=\begin{cases}\log m & m\in\mathbb{P}\\ 0 & \#\end{cases}$$

$$\begin{aligned}
F(\alpha)-\frac{\mu(q)}{\phi(q)}u(\beta) &= \sum_{p\le N}\log p . e(p\alpha) - \frac{\mu(q)}{\phi(q)}\sum_{m=1}^{N} e(m\beta) \\
&= \sum_{m=1}^{N}\lambda(m)e(m\alpha) - \frac{\mu(q)}{\phi(q)}\sum_{m=1}^{N} e(m\beta) \\
&= \sum_{m=1}^{N}\lambda(m)e(\frac{ma}{q}+m\beta) - \sum_{m=1}^{N}\frac{\mu(q)}{\phi(q)}e(m\beta) \\
&= \sum_{m=1}^{N}\Big(\lambda(m)e(\frac{ma}{q})-\frac{\mu(q)}{\phi(q)}\Big)e(m\beta)
\end{aligned}$$

طبق لم ۸ داریم

$$A(x):=\sum_{1\le m\le x}^{N}\Big(\lambda(m)e(\frac{ma}{q})-\frac{\mu(q)}{\phi(q)}\Big)$$

$$\begin{aligned}
A(x):=&\sum_{1\le m\le x}^{N}\lambda(m)e(\frac{ma}{q})-\frac{\mu(q)}{\phi(q)}x+O\big(\frac{1}{\phi(q)}\big) \\
=&F_x(\frac{a}{q})-\frac{\mu(q)}{\phi(q)}x+O(1)=O\big(\frac{QN}{(\log N)^C}\big)
\end{aligned}$$

در نتیجه

$$\begin{aligned}
F(\alpha)-\frac{\mu(q)}{\phi(q)}u(\beta) =&A(N)e(n\beta)-2\pi i\beta\int_1^N A(x)e(x\beta)\,\mathrm{d}x \\
\ll&|A(N)|+|\beta|N.\max\{A(x):1\le x\le N\} \\
\ll&\frac{Q^2N}{(\log N)^C}
\end{aligned}$$

برای قسمت بعدی لم توجه کنید که $|u(\beta)|<N$ و $C>2B$ نتیجه می‌دهد

$$\frac{Q^2N}{(\log N)^C}=\frac{N}{(\log N)^{C-2B}}<N$$

این دو به راحتی از به توان ۳ رساندن طرفین تقریبی که برای $F(\alpha)$ یافتیم، حکم موردنظر را نتیجه می‌دهند. □

قضیه ۱۰. *برای $B,C,\epsilon>0$ که $C>2B$، داریم*

$$\begin{aligned}
\int_M F(\alpha)^3e(-N\alpha)\,\mathrm{d}\alpha =&G(N)\frac{N^2}{2}+O\big(\frac{N^2}{(\log N)^{(1-\epsilon)B}}\big) \\
&+O\big(\frac{N^2}{(\log N)^{C-5B}}\big)
\end{aligned}$$

که ثابت‌های مورد نیاز فقط به B و C و ϵ وابسته هستند.

اثبات. ابتدا توجه کنید که اگر $q=1$، $M(q,a)$ بازه‌ای به طول $\frac{Q}{N}$ است و برای $q\ge 2$ بازه‌ای به طول $\frac{2Q}{N}$ است. با توجه به لم ۹ داریم

$$\begin{aligned}
&\int_M\big(F(\alpha)^3-\frac{\mu(q)}{\phi(q)}u(\alpha-\frac{a}{q})^3\big)e(-N\alpha)\,\mathrm{d}\alpha \\
&=\sum_{q\le Q}\sum_{\substack{a=0\\ (a,q)=1}}^{q}\int_{M(q,a)}\Big(F(\alpha)^3-\frac{\mu(q)}{\phi(q)}u(\alpha-\frac{a}{q})^3\Big)e(-N\alpha)\,\mathrm{d}\alpha \\
&\ll\sum_{q\le Q}\sum_{\substack{a=0\\ (a,q)=1}}^{q}\int_{M(q,a)}\frac{Q^2N^3}{(\log N)^C}\ll\sum_{q\le Q}\sum_{\substack{a=0\\ (a,q)=1}}^{q}\frac{Q^3N^2}{(\log N)^C} \\
&\ll\frac{Q^5N^2}{(\log)^C}=\frac{N^2}{(\log N)^{C-5B}}
\end{aligned}$$

اگر $\alpha = a/q+\beta \in M(q,a)$ آن‌گاه $|\beta| \le Q/N$ و داریم

$$\begin{aligned}
&\sum_{q\le Q}\sum_{\substack{a=0\\(a,q)=1}}^{q}\frac{\mu(q)}{\phi(q)^3}\int_{M(q,a)} u(\alpha-\frac{a}{q})^3 e(-N\alpha)\,\mathrm{d}\alpha\\
&=\sum_{q\le Q}\sum_{\substack{a=1\\(a,q)=1}}^{q}\frac{\mu(q)}{\phi(q)^3}\int_{\frac{a}{q}-\frac{Q}{N}}^{\frac{a}{q}+\frac{Q}{N}} u(\alpha-\frac{a}{q})^3 e(-N\alpha)\,\mathrm{d}\alpha\\
&=\sum_{q\le Q}\frac{\mu(q)}{\phi(q)^3}\sum_{\substack{a=1\\(a,q)=1}}^{q} e(-Na/q)\int_{-\frac{Q}{N}}^{\frac{Q}{N}} u(\beta)^3 e(-N\beta)\,\mathrm{d}\beta\\
&=\sum_{q\le Q}\frac{\mu(q)c_q(-N)}{\phi(q)^3}\int_{-Q/N}^{Q/N} u(\beta)^3 e(-N\beta)\,\mathrm{d}\beta\\
&=G(N,Q)\int_{-\frac{Q}{N}}^{\frac{Q}{N}} u(\beta)^3 e(-N\beta)\,\mathrm{d}\beta
\end{aligned}$$

طبق لم ۶ اگر $|\beta| \le \frac{1}{2}$، آن‌گاه $u(\beta) \ll |\beta|^{-1}$ و در نتیجه

$$\begin{aligned}
\int_{\frac{Q}{N}}^{\frac{1}{2}} u(\beta)^3 e(-N\beta)\,\mathrm{d}\beta &\ll \int_{\frac{Q}{N}}^{\frac{1}{2}} |u(\beta)|^3\,\mathrm{d}\beta\\
&\ll \int_{\frac{Q}{N}}^{\frac{1}{2}} \beta^{-3}\,\mathrm{d}\beta < \frac{N^2}{Q^2}\\
\xRightarrow{\text{مشابها}} \int_{-\frac{1}{2}}^{-\frac{Q}{N}} u(\beta)^3 e(-N\beta)\,\mathrm{d}\beta &\ll \frac{N^2}{Q^2}
\end{aligned}$$

طبق لم ۴ داریم

$$\begin{aligned}
\int_{-\frac{Q}{N}}^{\frac{Q}{N}} u(\beta)^3 e(-N\beta)\,\mathrm{d}\beta &= \int_{\frac{1}{2}}^{\frac{1}{2}} u(\beta)^3 e(-N\beta)\,\mathrm{d}\beta + O(\frac{N^2}{Q^2})\\
&=\frac{N^2}{Q^2}+O(N)+O(\frac{N^2}{Q^2})\\
&=\frac{N^2}{2}+O(\frac{N^2}{Q^2})
\end{aligned}$$

طبق قضیه ۳ داریم $G(N,Q) = G(N) + O(\frac{1}{Q^{1-\epsilon}})$. با توجه به نکات گفته شده می‌توان نوشت

$$\begin{aligned}
\int_M F(\alpha)^3 e(-N\alpha)\,\mathrm{d}\alpha =&G(N,Q)\int_{-\frac{Q}{N}}^{\frac{Q}{N}} u(\beta)^3 e(-N\beta)\,\mathrm{d}\beta\\
&+O(\frac{N^2}{(\log N)^{C-5B}})\\
=&G(N)\frac{N^2}{2}+O(\frac{N^2}{Q^{1-\epsilon}})\\
&+O(\frac{N^2}{(\log N)^{C-5B}})\\
=&G(N)\frac{N^2}{2}+O(\frac{N^2}{(\log N)^{(1-\epsilon)B}})\\
&+O(\frac{N^2}{(\log N)^{C-5B}})
\end{aligned}$$

به این ترتیب حکم مورد نظر اثبات شد. $\square$

۶ محاسبه‌ی انتگرال روی m

قضیه ۱۱. (*Vinogradov*) *a و q اعدادی طبیعی هستند طوری که $1 \le q \le N$ و $(a,q)=1$. اگر $|\alpha-a/q| \le \frac{1}{q^2}$، آن‌گاه داریم*

$$F(\alpha) \ll (\frac{N}{\sqrt{q}}+N^{\frac{4}{5}}+\sqrt{Nq})(\log N)^4$$

قضیه ۱۱ به راحتی تقریب مورد نیاز ما را برای انتگرال روی m به دست می‌دهد. اثبات این قضیه دشوار را طی ۴ لم بعدی به دست می‌آوریم.

لم ۱۲. (*Vaughan's identity*) *برای $u \ge 1$ تعریف می‌کنیم $M_u(k) = \sum_{d|k}\mu(d)$. فرض کنید $\phi(k,l)$ یک تابع حسابی دو متغیره باشد. در این صورت رابطه‌ی زیر برقرار است.*

$$\begin{aligned}
&\sum_{u<l\le N}\phi(1,l)+\sum_{u<k\le N}\sum_{u<l\le\frac{N}{k}} M_u(k)\phi(k,l)\\
=&\sum_{d\le u}\sum_{u<l\le\frac{N}{d}}\sum_{m\le\frac{N}{ld}}\mu(d)\phi(dm,l)
\end{aligned}$$

اثبات. جمع زیر را به دو روش محاسبه می‌کنیم

$$S=\sum_{k=1}^{N}\sum_{u<\le\frac{N}{K}} M_u(k)\phi(k,l)$$

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

$$\Rightarrow M_u(k)=\begin{cases}1 & k=1\\ 0 & 1\leq k\leq u\end{cases}$$

$$\Rightarrow S=\sum_{u<l\leq N}\phi(1,l)+\sum_{u<k\leq N}\sum_{u<l\leq \frac{N}{k}}M_u(k)\phi(k,l)$$

از طرف دیگر با تغییر متغیر $k=dm$ نتیجه می‌شود.

$$\begin{aligned}S&=\sum_{k=1}^{N}\sum_{u<l\leq \frac{N}{k}}\sum_{\substack{d|k\\ d\leq u}}\mu(d)\phi(k,l)\\ &=\sum_{d\leq u}\sum_{\substack{k=1\\ d|k}}^{N}\sum_{u<l\leq \frac{N}{k}}\mu(d)\phi(k,l)\\ &=\sum_{d\leq u}\sum_{m\leq \frac{N}{d}}\sum_{u<l\leq \frac{N}{dm}}\mu(d)\phi(dm,l)\\ &=\sum_{d\leq u}\sum_{u<l\leq \frac{N}{d}}\sum_{m\leq \frac{N}{ld}}\mu(d)\phi(dm,l)\end{aligned}$$

دو رابطه‌ی فوق حکم موردنظر را نتیجه می‌دهند. □

لم ۱۳. *فرض کنید Λ تابع منگولت باشد. در این صورت برای هر α داریم*

$$F(\alpha)=S_1-S_2-S_3+O(\sqrt{N})$$

که در آن

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

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

$$S_3=\sum_{k>N^{\frac{2}{5}}}\sum_{N^{\frac{2}{5}}<l\leq \frac{N}{k}}M_{N^{\frac{2}{5}}}(k)\Lambda(l)e(\alpha kl)$$

اثبات. برای اثبات از لم ۱۲ استفاده می‌کنیم. قرار می‌دهیم $\phi(k,l)=\Lambda(l)e(\alpha kl)$ و $u=N^{\frac{2}{5}}$ جملاتی را که در لم ۱۲ ظاهر می‌شوند، محاسبه می‌کنیم.

$$\begin{aligned}\sum_{u<l\leq N}\phi(1,l)&=\sum_{N^{\frac{2}{5}}<l\leq N}\Lambda(l)e(\alpha l)\\ &=\sum_{l=1}^{N}\Lambda(l)e(\alpha l)-\sum_{l\leq N^{\frac{2}{5}}}\Lambda(l)e(\alpha l)\\ &=\sum_{p^k\leq N}\log p.e(\alpha p^k)+O(N^{\frac{2}{5}}\log N)\\ &=\sum_{p\leq N}\log p.e(p\alpha)+\sum_{\substack{p^k\leq N\\ k\geq 2}}\log p.e(p^k\alpha)\\ &\qquad+O(N^{\frac{2}{5}}\log N)\\ &=F(\alpha)+O\Big(\sum_{\substack{p^k\leq N\\ k\geq 2}}\log N\Big)+O\big(N^{\frac{2}{5}}\log N\big)\\ &=F(\alpha)+O\Big(\sum_{p^2\leq N}\lfloor\frac{\log N}{\log p}\rfloor\Big)+O\big(N^{\frac{2}{5}}\log N\big)\\ &=F(\alpha)+O\Big(\pi(\sqrt{N})\log N\Big)+O\big(N^{\frac{2}{5}}\log N\big)\\ &=F(\alpha)+O(\sqrt{N})\end{aligned}$$

در تساوی آخر از این استفاده کردیم که $\pi(\sqrt{N})\log N \ll \sqrt{N}$ (این نتیجه‌ای از قضیه‌ی چبیشف است).

$$\begin{aligned}\sum_{u<k\leq N}\sum_{u<l\leq \frac{N}{k}}M_u(k)\phi(k,d)&\\ =\sum_{N^{\frac{2}{5}}<k\leq N}\sum_{N^{\frac{2}{5}}<l\leq \frac{N}{k}}M_{N^{\frac{2}{5}}}(k)\Lambda(l)e(\alpha kl)&=S_3\end{aligned}$$

$$\begin{aligned}\sum_{d\leq u}\sum_{u<l\leq \frac{N}{d}}\sum_{m\leq \frac{N}{ld}}\mu(d)\phi(dm,l)&\\ =\sum_{d\leq N^{\frac{2}{5}}}\sum_{N^{\frac{2}{5}}<l\leq \frac{N}{d}}\sum_{m\leq \frac{N}{ld}}\mu(d)\Lambda(l)e(\alpha dlm)&\\ =\sum_{d\leq N^{\frac{2}{5}}}\sum_{l\leq \frac{N}{d}}\sum_{m\leq \frac{N}{ld}}\mu(d)\Lambda(l)e(\alpha dlm)&\\ -\sum_{d\leq N^{\frac{2}{5}}}\sum_{l\leq N^{\frac{2}{5}}}\sum_{m\leq \frac{N}{ld}}\mu(d)\Lambda(l)e(\alpha dlm)&=S_1-S_2\end{aligned}$$

با جایگذاری روابط فوق در اتحاد بیان شده در لم ۱۲ حکم نتیجه می‌شود. □

در ادامه می‌خواهیم برای S_1 و S_2 و S_3 کران بالا به دست آوریم.

لم ۱۴. *با فرض‌های قضیه ۱۱ داریم*

$$|S_1| \ll \Big(\frac{N}{q} + N^{\frac{2}{5}} + q\Big)(\log N)^2$$

اثبات. فرض کنید $u = N^{\frac{2}{5}}$. می‌دانیم $\sum_{l|r}\Lambda(l) = \log r$. داریم

$$\begin{aligned}
S_1 &= \sum_{d\le u}\sum_{l\le \frac{N}{d}}\sum_{m\le \frac{N}{ld}} \mu(d)\Lambda(l)e(\alpha dlm)\\
&= \sum_{d\le u}\sum_{lm\le \frac{N}{d}} \mu(d)\Lambda(l)e(\alpha dlm)\\
&= \sum_{d\le u}\sum_{r\le \frac{N}{d}} \mu(d)e(\alpha dr)\sum_{l|r}\Lambda(l)\\
&= \sum_{d\le u}\mu(d)\sum_{r\le \frac{N}{d}} e(\alpha dr)\log r\\
&\ll \sum_{d\le u}\mu(d)\Big|\sum_{r\le \frac{N}{d}} e(\alpha dr)\log r\Big|
\end{aligned}$$

اکنون جمع داخل قدر مطلق را محاسبه می‌کنیم.

$$\begin{aligned}
\sum_{r\le \frac{N}{d}} e(\alpha dr)\log r &= \sum_{r\le \frac{N}{d}} e(\alpha dr)\int_1^r \frac{\mathrm{d}x}{x}\\
&= \sum_{r=2}^{\lfloor \frac{N}{d}\rfloor} e(\alpha dr)\sum_{s=2}^{r}\int_{s-1}^{s}\frac{\mathrm{d}x}{x}\\
&= \sum_{s=2}^{\lfloor \frac{N}{d}\rfloor}\sum_{r=s}^{\lfloor \frac{N}{d}\rfloor}\int_{s-1}^{s} e(\alpha dr)\frac{\mathrm{d}x}{x}\\
&= \sum_{s=2}^{\lfloor \frac{N}{d}\rfloor}\int_{s-1}^{s}\Big(\sum_{s=2}^{\lfloor \frac{N}{d}\rfloor} e(\alpha dr)\Big)\frac{\mathrm{d}x}{x}
\end{aligned}$$

طبق لم ۶ داریم

$$\begin{aligned}
&\sum_{r=s}^{\lfloor \frac{N}{d}\rfloor} e(dr\alpha) \ll \min\{\frac{N}{d}, \|\alpha d\|^{-1}\}\\
\Rightarrow &\sum_{r\le \frac{N}{d}} e(dr\alpha)\log r \ll \min\{\frac{N}{d}, \|\alpha d\|^{-1}\}\log N\\
\Rightarrow &S_1 \ll \min\{\frac{N}{d}, \|\alpha d\|^{-1}\}\log N
\end{aligned}$$

در این‌جا از حکمی استفاده می‌کنیم که اثبات آن در ضمیمه آمده است. این حکم بیان می‌کند: اگر $\alpha \in \mathbb{R}$ و $|\alpha - \frac{a}{q}| \le \frac{1}{q^2}$ که در آن $a, q \in \mathbb{Z}$ و $q \ge 1$ و $(a,q) = 1$ به ازای هر $n \in \mathbb{N}$ و $U \ge 1$ داریم

$$\sum_{1\le k\le U}\min\{\frac{n}{k}, \|\alpha k\|^{-1}\} \ll \Big(\frac{n}{q} + U + q\Big)\log(2qU) \qquad (2)$$

در نتیجه در این‌جا می‌توان نوشت

$$\sum_{n\le d}\min\{\frac{N}{d}, \|\alpha k\|^{-1}\} \ll \Big(\frac{N}{q} + N^{\frac{2}{5}} + q\Big)\log N$$

دو رابطه‌ی فوق حکم مورد نظر را نتیجه می‌دهند. □

لم ۱۵. *با فرض‌های قضیه ۱۱ داریم*

$$|S_2| \ll \Big(\frac{N}{q} + N^{\frac{4}{5}} + q\Big)(\log N)^2$$

اثبات. اگر $d \le N^{\frac{2}{5}}$ و $l \le N^{\frac{2}{5}}$ آن‌گاه $dl \le N^{\frac{4}{5}}$. در نتیجه با تغییر متغیر $k = dl$ داریم

$$\begin{aligned}
S_2 &= \sum_{d\le N^{\frac{2}{5}}}\sum_{l\le N^{\frac{2}{5}}}\sum_{m\le \frac{N}{ld}} \mu(d)\Lambda(l)e(\alpha dlm)\\
&= \sum_{k\le N^{\frac{4}{5}}}\Big(\sum_{k\le \frac{N}{k}} e(\alpha km)\Big)\Big(\sum_{\substack{k=dl\\ d,l\le N^{\frac{2}{5}}}} \mu(d)\Lambda(l)\Big)
\end{aligned}$$

همچنین داریم

$$\begin{aligned}
\sum_{\substack{k=dl\\ d,l\le N^{\frac{2}{5}}}} \mu(d)\Lambda(l) &\ll \sum_{\substack{k=dl\\ d,l\le N^{\frac{2}{5}}}} \Lambda(l)\\
&\le \sum_{l|k}\Lambda(l) = \log k \ll \log N
\end{aligned}$$

اکنون مشابه لم قبل با استفاده از لم ۶ و حکم (۲) نتیجه می‌شود

$$\begin{aligned}
S_2 &\ll \log N \sum_{k\le N^{\frac{4}{5}}}\sum_{m\le \frac{N}{k}} e(\alpha km)\\
&\ll \log N \sum_{k\le N^{\frac{4}{5}}}\min\{\frac{N}{k}, \|\alpha k\|^{-1}\}\\
&\ll \Big(\frac{N}{q} + N^{\frac{4}{5}} + q\Big)(\log N)^2
\end{aligned}$$

اثبات لم به پایان رسید. □

لم ۱۶. *با فرض‌های قضیه ۱۱ داریم*

$$|S_3| \ll \Big(\frac{N}{\sqrt{q}} + N^{\frac{4}{5}} + \sqrt{Nq}\Big)(\log N)^4$$

اثبات. قرار می‌دهیم $u = N^{\frac{2}{5}}$ و $h = \lfloor \frac{\log N}{2\log 2}\rfloor + 1$. در این صورت $N^{\frac{1}{5}} < 2^h \le 2N^{\frac{1}{5}}$ و $h \ll \log N$. اگر $ileh$ آن‌گاه $2^i u \le 2N^{\frac{3}{5}} \ll N$. اگر $N^{\frac{2}{5}} < l \le \frac{N}{k}$ آن‌گاه

$$k \le \frac{N}{d} < N^{\frac{3}{5}} = N^{\frac{1}{5}}u < 2^h u$$

در نتیجه می‌توان نوشت

$$S_3=\sum_{k>N^{\frac{2}{5}}}\sum_{N^{\frac{2}{5}}<l\le\frac{N}{k}}M_u(k)\Lambda(l)e(\alpha kl)$$
$$=\sum_{i=1}^{h}\sum_{2^{i-1}u<k\le 2^iu}M_u(k)\sum_{u<l\le\frac{N}{k}}\Lambda(d)e(\alpha kl)=\sum_{i=1}^{h}S_{3,i}$$

که در آن

$$S_{3,i}=\sum_{2^{i-1}u<k\le 2^iu}M_u(k)\sum_{u<l\le\frac{N}{k}}\Lambda(d)e(\alpha kl)$$

از نابرابری کوشی-شوارتز نتیجه می‌شود

$$|S_{3,i}|^2\le\Big(\sum_{2^{i-1}<k\le 2^iu}|M_u(k)|^2\Big).$$
$$\Big(\sum_{2^{i-1}<k\le 2^iu}\Big|\sum_{u<l\le\frac{N}{k}}\Lambda(l)e(\alpha kl)\Big|^2\Big)$$

اکنون می‌خواهیم برای دو عبارت فوق کران بالا پیدا کنیم.

$$|M_u(k)|=\Big|\sum_{\substack{d|k\\ d\le u}}\mu(d)\Big|\le\sum_{\substack{d|k\\ d\le u}}1\le d(k)$$

که $d(n)$ تعداد مقسوم‌علیه‌های مثبت n است. در این جا از حکم دیگری که در ضمیمه اثبات می‌کنیم، استفاده می‌کنیم. این حکم بیان می‌کند

$$\sum_{n\le x}d(n)^2\ll x(\log x)^3 \qquad (3)$$

در نتیجه داریم

$$\sum_{2^{i-1}<k\le 2^iu}|M_u(k)|^2\le\sum_{2^{i-1}<k\le 2^iu}d(k)^2\ll 2^iu(\log 2^iu)^3$$
$$\ll 2^iu(\log N)^3$$

کران موردنیاز برای عبارت اول به دست آمد. به سراغ عبارت دوم می‌رویم

$$\sum_{2^{i-1}<k\le 2^iu}\Big|\sum_{u<l\le\frac{N}{k}}\Lambda(l)e(\alpha kl)\Big|^2$$
$$=\sum_{2^{i-1}<k\le 2^iu}\sum_{u<l\le\frac{N}{k}}\sum_{u<m\le\frac{N}{k}}\Lambda(l)\lambda(m)e(\alpha k(l-m))$$
$$=\sum_{u<l<\frac{N}{2^{i-1}u}}\sum_{u<m<\frac{N}{2^{i-1}u}}\Lambda(l)\lambda(m)\sum_{k\in I(k,m)}e(\alpha k(l-m))$$

که در این‌جا

$$I(l,m)=\{k\in\mathbb{Z}|2^{i-1}u<k\le\min\{2^iu,\frac{N}{l},\frac{N}{m}\}\}$$

به وضوح داریم $|I(l,m)|\le 2^{i-1}u$ در نتیجه طبق لم ۶ داریم

$$\sum_{k\in I(l,m)}e\big(\alpha k(l-m)\big)\ll\min\{2^{i-1}u,\|\alpha(l-m)\|^{-1}\}$$

به ازای اعداد صحیح $l,m\in[1,N]$ داریم $\Lambda(m)\le\log N$ و $0\le\Lambda(l)$. در نتیجه داریم

$$\sum_{2^{i-1}u<k\le 2^iu}\Big|\sum_{u<l\le\frac{N}{k}}\Lambda(l)e(\alpha kl)\Big|^2$$
$$\ll\sum_{u<l<\frac{N}{2^{i-1}u}}\sum_{u<m<\frac{N}{2^{i-1}u}}\Lambda(l)\Lambda(m)Z$$
$$\ll(\log N)^2\sum_{u<l<\frac{N}{2^{i-1}u}}\sum_{u<m<\frac{N}{2^{i-1}u}}\Lambda(l)\Lambda(m)Z$$

که در آن

$$Z=\min\{2^{i-1}u,\|\alpha(l-m)\|^{-1}\}$$

قرار می‌دهیم $j=l-m$ که $m<\frac{N}{2^{i-1}u}$ و $u<l$. در این صورت $|j|<\frac{N}{2^{i-1}}u$ و تعداد راه‌های نمایش چنین jای به شکل مذکور حداکثر $\frac{N}{2^{i-1}u}$ است. با توجه به حکم (۲) داریم

$$\sum_{2^{i-1}u<k\le M2^iu}\Big|\sum_{u<l\le\frac{N}{k}}\Lambda(l)e(\alpha kl)\Big|^2$$
$$\ll(\log N)^2\frac{N}{2^{i-1}u}\sum_{i\le j\le\frac{N}{2^{i-1}u}}\min\{2^{i-1}u,\|\alpha j\|^{-1}\}$$
$$\ll(\log N)^2\frac{N}{2^{i-1}u}\sum_{i\le j\le\frac{N}{2^{i-1}u}}\min\{\frac{N}{j},\|\alpha j\|^{-1}\}$$
$$\ll\frac{N}{2^{i-1}u}\Big(\frac{N}{q}+\frac{N}{2^{i-1}u}+q\Big)(\log N)^3$$

دومین کران موردنیاز را به دست آوردیم. اکنون می‌توانیم یک کران برای $S_{3,i}$ پیدا کنیم.

$$|S_{3,i}|^3\ll\big(2^iu(\log N)^3\big)\frac{N}{2^{i-1}u}\Big(\frac{N}{q}+\frac{N}{2^{i-1}u}+q\Big)(\log N)^3$$
$$\ll N^2(\log N)^6\Big(\frac{1}{q}+\frac{1}{u}+\frac{q}{N}\Big)$$
$$\le N^2(\log N)^6\Big(\frac{1}{\sqrt{q}}+\frac{1}{\sqrt{u}}+\sqrt{\frac{q}{N}}\Big)^2$$
$$\Rightarrow|S_{3,i}|\ll N(\log N)^3\Big(\frac{1}{\sqrt{q}}+\frac{1}{N^{\frac{1}{5}}}+\sqrt{\frac{q}{N}}\Big)$$

$$h\ll\log N\Rightarrow S_3=\sum_{i=1}^{h}S_{3,i}\ll(\log N)^4\Big(\frac{N}{\sqrt{q}}+N^{\frac{4}{5}}+\sqrt{q}N\Big)$$

این اثبات لم را کامل می‌کند. □

اکنون کافی است کران‌هایی را که برای S_1 و S_2 و S_3 یافتیم در لم ۱۳ جایگذاری کنیم تا به حکم قضیه ۱۱ برسیم. اکنون آماده‌ایم تا مقدار انتگرال روی m را به کمک قضیه ۱۱ تقریب بزنیم.

قضیه ۱۷. *برای هر $B > 0$ داریم*

$$\int_m F(\alpha)^3 e(-N\alpha)\,\mathrm{d}\alpha \ll \frac{N^2}{(\log N)^{\frac{B}{2}-5}}$$

که ثابت مورد (برای $\ll$) فقط به B وابسته است.

اثبات. $\alpha \in m$ را در نظر می‌گیریم. طبق قضیه‌ی دیریکله (که در ضمیمه بیان و اثبات شده است.) عدد گویای $\frac{a}{q} \in [0,1]$ با شرط $1 \le q \le N/Q$ و $(a,q)=1$ موجود است که

$$|\alpha - \frac{a}{q}| \le \frac{Q}{q^N} \le \min\{Q/N, 1/q^2\}$$

اگر $q \le Q$ باشد نتیجه می‌شود $\alpha \in M(q,a)$ که امکان ندارد (چون $\alpha \in m$). در نتیجه درایم $Q < q \le N/Q$. طبق قضیه‌ی ۱۱ داریم:

$$\begin{aligned}
F(\alpha) &\ll (\frac{N}{\sqrt{q}} + N^{4/5} + \sqrt{Nq})(\log N)^4 \\
&\ll (\frac{N}{(\log N)^{B/2}} + N^{4/5} + \sqrt{N}(\frac{N}{(\log N)^B})^{1/2})(\log N)^4 \\
&\ll \frac{N}{(\log N)^{B/2-4}}
\end{aligned}$$

طبق قضیه چبیشف داریم:

$$\begin{aligned}
v(N) &:= \sum_{p \le N} \log p \\
&\le \pi(N)\log N \ll N \\
&\Rightarrow \int_0^1 |F(\alpha)|^2 \mathrm{d}\alpha \\
&= \sum_{p \le N} (\log p)^2 \\
&\le \log N \sum_{p \le N} \log p \\
&= \log N . v(N) lN \log N \\
&\Rightarrow \int_m |F(\alpha)|^3 \mathrm{d}\alpha \\
&\ll \sup\{|F(\alpha)| : \alpha \in m\} \int_m |F(\alpha)|^2 \mathrm{d}\alpha \\
&\ll \frac{N}{(\log N)^{B/2-4}} \int_0^1 |F(\alpha)|^2 \mathrm{d}\alpha \\
&\ll \frac{N^2}{(\log N)^{B/2-5}}
\end{aligned}$$

اثبات کامل شد. □

۷ اثبات قضیه ۱

در این قسمت ابتدا یک تخمین برای $R(N)$ به دست می‌آوریم و سپس با استفاده از آن قضیه ۱ را اثبات می‌کنیم.

قضیه ۱۸. (*Vinogradov*) *برای N فرد به اندازه‌ی کافی بزرگ و برای هر $A > 0$ داریم*

$$R(N) = G(N)\frac{N^2}{2} + O(\frac{N^2}{(\log N)^A})$$

که ثابت مورد نیاز فقط به A وابسته است.

اثبات. از قضیه‌های ۱۰ و ۱۷ نتیجه می‌شود برای هر $B, C, \epsilon > 0$ که $C > 2B$ داریم

$$\begin{aligned}
R(N) &= \int_0^1 F(\alpha)^3 e(-N\alpha)\mathrm{d}\alpha \\
&= \int_M F(\alpha)^3 e(-N\alpha)\mathrm{d}\alpha + \int_m F(\alpha)^3 e(-N\alpha)\mathrm{d}\alpha \\
&= G(N)\frac{N^2}{2} + O(\frac{N^2}{(\log N)^{(1-\epsilon)B}}) + O(\frac{N^2}{(\log N)^{C-5B}}) \\
&+ O(\frac{N^2}{(\log N)^{B/2-5}})
\end{aligned}$$

که ثابت‌های مورد نیاز فقط به B و C و ϵ وابسته هستند. اکنون قرار می‌دهیم:

$$B = 2A + 10, C = A + 5B, \epsilon = \frac{1}{2}$$

با توجه به اینکه $A = \min\{(1-\epsilon)B, C-5B, B/2-5\}$، با جایگذاری در رابطه‌ی فوق به دست می‌آوریم

$$R(N) = G(N)\frac{N^2}{2} + O(\frac{N^2}{(\log N)^A}($$

و ثابت مورد نیاز فقط به A بستگی دارد. □

اثبات قضیه ۱: ابتدا توجه کنید که داریم

$$\begin{aligned}
R(N) &= \sum_{p_1+p_2+p_3=N} \log p_1 \log p_2 \log p_3 \\
&\le (\log N)^3 \sum_{p_1+p_2+p_3=N} 1 = (\log N)^3 . r(N)
\end{aligned}$$

به ازای $0 < \delta < \frac{1}{2}$ فرض کنید $r_\delta(N)$ برابر تعداد نمایش‌های N به صورت $N = p_1 + p_2 + p_3$ با شرط $\exists i : p_i \le N^{1-\delta}$ باشد. در این صورت داریم:

$$\begin{aligned}
r_\delta(N) &\ll 3 \sum_{p_1+p_2+p_3=N, p_1 \le N^{1-\delta}} 1 \ll \sum_{p_1 \le N^{1-\delta}} (\sum_{p_2+p_3=N-p_1} 1) \\
&\le \sum_{p_1 \le N^{1-\delta}} (\sum_{p_2 < N} 1) \\
&\le \pi(N^{1-\delta})\pi(N) \ll \frac{N^{2-\delta}}{(\log N)^2}
\end{aligned}$$

با توجه به این نکته می‌توان نوشت:

$$\begin{aligned}
R(N) &\ge \sum_{p_1+p_2+p_3=N,\, p_1,p_2,p_3>N^{1-\delta}} \log p_1.\log p_2.\log p_3 \\
&\ge (1-\delta)^3(\log N)^3\Big(\sum_{p_1+p_2+p_3=N,\, p_1,p_2,p_3>N^{1-\delta}} 1\Big) \\
&\ge (1-\delta)^3(\log N)^3(r(N)-r_\delta(N)) \\
&\gg (1-\delta)^3(\log N)^3\Big(r(N)-\frac{N^{2-\delta}}{(\log N)^2}\Big) \\
&\Rightarrow (\log N)^3 r(N) \le (1-\delta)^{-3}R(N) + (\log N)N^{2-\delta}
\end{aligned}$$

$$0<\delta<\frac{1}{2} \Rightarrow \frac{1}{2} < 1-\delta < 1$$

$$\Rightarrow 0 < (1-\delta)^{-3}-1 = \frac{1-(1-\delta)^3}{(1-\delta)^3} \le 8(1-(1-\delta)^3) < 24\delta$$

طبق قضیه ۱۸، $R(N)\ll N^2$ و در نتیجه داریم:

$$\begin{aligned}
0 &\le (\log N)^3 r(N) - R(N) \\
&\le ((1-\delta)^{-3}-1)R(N) + (\log N)N^{2-\delta} \\
&\ll \delta R(N) + (\log N)N^{2-\delta} \\
&\ll \delta N^2 + (\log N)N^{2-\delta} = N^2\Big(\delta + \frac{\log N}{N^\delta}\Big)
\end{aligned}$$

این نابرابری برای هر $\delta\in(0,\frac{1}{2})$ برقرار است و ثابت مورد نیاز به δ بستگی ندارد. قرار می‌دهیم:

$$\begin{aligned}
\delta &= \frac{2\log\log N}{\log N} \\
&\Rightarrow \delta + \frac{\log N}{N^\delta} = \frac{2\log\log N}{\log N} + \frac{\log N}{(\log N)^2} << \frac{\log\log N}{\log N} \\
&\Rightarrow 0 \le (\log N)^3 r(N) - R(N) \ll \frac{N^2\log\log N}{\log N}
\end{aligned}$$

فرض کنید $A\ge 1$. طبق قضیه ۱۸ داریم:

$$\begin{aligned}
(\log N)^3 r(N) &= R(N) + O\Big(\frac{N^2\log\log N}{\log N}\Big) \\
&= G(N)\frac{N}{2} + O\Big(\frac{N^2}{(\log N)^A}\Big) \\
&\quad + O\Big(\frac{N^2\log\log N}{\log N}\Big) \\
&= G(N)\frac{N^2}{2}\Big(1+O\Big(\frac{N^2\log\log N}{\log N}\Big)\Big) \\
\Rightarrow r(N) &= G(N)\frac{N^2}{2(\log N)^3}\Big(1+O\Big(\frac{N^2\log\log N}{\log N}\Big)\Big)
\end{aligned}$$

به این ترتیب اثبات قضیه کامل می‌شود.

۸ ضمیمه

در این‌جا چند حکم را که در اثبات‌ها به کار بردیم ولی به منظور جلوگیری از انحراف از موضوع آن‌ها را اثبات نکردیم، بیان و اثبات خواهیم کرد.

(i)

فرض کنید α عددی حقیقی باشد. اگر $|\alpha - \frac{a}{q}| \le \frac{1}{q^2}$ که در آن $a,q\in\mathbb{Z}$ و $q\ge 1$ و $(a,q)=1$ آن‌گاه برای هر عدد حقیقی $U\ge 1$ و عدد طبیعی n داریم

$$\sum_{1\le k\le U}\min\{\frac{n}{k}, ||\alpha k||^{-1}\} \ll \Big(\frac{n}{q}+U+q\Big)\log(2qU)$$

برای اثبات به دو لم نیاز داریم!

لم ۱۹. *با فرض‌های (i)، داریم:*

$$\sum_{1\le r\le \frac{q}{2}} ||\alpha r||^{-1} \ll q\log q$$

اثبات. حکم برای $q=1$ واضح است. پس فرض می‌کنیم $q\ge 2$. برای هر عدد صحیح r، اعداد صحیح $m(r), s(r)\in[0,\frac{q}{2}]$ موجود است به طوری که داریم:

$$\frac{s(r)}{q} = ||\frac{ar}{q}|| = \pm\Big(\frac{ar}{q}-m(r)\Big)$$

چون $(a,q)=1$ داریم

$$s(r)=0 \iff r\equiv 0 \pmod{q}$$

در نتیجه وقتی $r\in[1,\frac{q}{2}]$ آن‌گاه $s(r)\in[1,\frac{q}{2}]$. قرار می‌دهیم:

$$\theta := q^2\Big(\alpha-\frac{a}{q}\Big) \Rightarrow -1\le\theta\le 1$$

در نتیجه عدد حقیقی θ' موجود است که:

$$\alpha r := \frac{ar}{q}+\frac{\theta r}{q^2} = \frac{ar}{q}+\frac{\theta'}{2q}$$

در نتیجه داریم:

$$|\theta'| = |\frac{2\theta r}{q}| \le |\theta| \le 1$$

با توجه به آن‌چه گفتیم می‌توان نوشت:

$$\begin{aligned}
||\alpha r|| &= ||\frac{ar}{q}+\frac{\theta'}{2q}|| \\
&= ||m(r)\pm\frac{s(r)}{q}+\frac{\theta'}{2q}|| \\
&= ||\frac{s(r)}{q}\pm\frac{\theta'}{2q}|| \\
&\ge ||\frac{s(r)}{q}|| - ||\frac{\theta'}{2q}|| \\
&\ge \frac{s(r)}{q} - \frac{1}{2q} \ge \frac{1}{2q}
\end{aligned}$$

ادعا می‌کنیم برای $1\le r_1\le r_2\le \frac{q}{2}$ داریم

$$s(r_1)=s(r_2) \iff r_1=r_2$$

داریم

$$\begin{aligned}
&s(r_1)=s(r_2)\\
&\Rightarrow ||\frac{ar_2}{q}||=||\frac{ar_2}{q}||\\
&\Rightarrow \pm(\frac{ar_1}{q}-m(r_1))=\pm(\frac{ar_2}{q}-m(r_2))\\
&\Rightarrow ar_1\equiv \pm ar_2(\mod q)
\end{aligned}$$

$$(a,q)=1\Rightarrow r_1\equiv \pm r_2(\mod q)$$

$$1\leq r_1\leq r_2\leq \frac{q}{2}\Rightarrow r_1=r_2$$

ادعایمان را اثبات کردیم. از این ادعا می‌توان نتیجه گرفت

$$\begin{aligned}
&\{||\frac{ar}{q}||:1\leq r\leq \frac{q}{2}\}\\
&=\{\frac{s(r)}{q}:1\leq r\leq \frac{q}{2}\}\\
&=\{\frac{s}{q}:1\leq s\leq \frac{q}{2}\}
\end{aligned}$$

در نتیجه می‌توان نوشت:

$$\begin{aligned}
\sum_{1\leq r\leq \frac{q}{2}}||\alpha r||^{-1}&\leq \sum_{1\leq r\leq \frac{q}{2}}(\frac{s(r)}{q}-\frac{1}{2q})^{-1}\\
&=\sum_{1\leq s\leq \frac{q}{2}}(\frac{s}{q}-\frac{1}{2q})^{-1}\\
&=2q\sum_{1\leq s\leq \frac{q}{2}}\frac{1}{2s-1}\\
&\leq 2q\sum_{1\leq s\leq \frac{q}{2}}\frac{1}{s}\ll q\log q
\end{aligned}$$

حکم اثبات شد. □

لم ۲۰. *با فرض‌های (i)، برای هر عدد حقیقی و مثبت V و عدد صحیح نامنفی h داریم:*

$$\sum_{r=1}^{q}\min\{V,||\alpha(hq+r)^{-1}||\}\ll V+q\log q$$

اثبات. فرض کنید $\theta\in[-1,1]$ طوری باشد که $\alpha=\frac{a}{q}+\frac{\theta}{q^2}$. در این صورت داریم

$$\begin{aligned}
\alpha(hq+r)&=ah+\frac{ar}{q}+\frac{\theta h}{q}+\frac{\theta r}{q^2}\\
&=ah+\frac{ar}{q}+\frac{\lfloor\theta h\rfloor+\{\theta h\}}{q}+\frac{\theta r}{q^2}\\
&=ah+\frac{ar+\lfloor\theta h\rfloor+\delta(r)}{q}
\end{aligned}$$

که در آن $2>\{\theta h\}+\frac{\theta r}{q}=\delta(r)\leq -1$. برای هر $r\in\{1,2,\dots,q\}$ عدد صحیح یکتای r' موجود است که

$$\{\alpha(hq+r)\}=\frac{ar+\lfloor\theta h\rfloor+\delta(r)}{q}-r'$$

اگر $t\leq\{\alpha(hq+r)\}\leq t+\frac{1}{q}$ آن‌گاه:

$$\begin{aligned}
&qt\leq ar-qr'+\lfloor\theta h\rfloor+\delta(r)\leq qt+1\\
&\Rightarrow ar-qr'\leq qt-\lfloor\theta h\rfloor+1-\delta(r)\leq qt-\lfloor\theta h\rfloor+2
\end{aligned}$$

همچنین می‌توان نتیجه گرفت

$$\begin{aligned}
&ar-qr'\geq qt-\lfloor\theta h\rfloor-\delta(r)>qt-\lfloor\theta h\rfloor-2\\
&\Rightarrow ar-qr'\in J=(qt-\lfloor\theta h\rfloor-2,qt-\lfloor\theta h\rfloor+2]\\
&\Rightarrow |J|=4
\end{aligned}$$

بازه‌ی J شامل دقیقا چهار عدد صحیح است. برای $1\leq r_1\leq r_2\leq q$ داریم

$$\begin{aligned}
&ar_1-qr_1'=ar_2-qr_2'\\
&\Rightarrow ar_1\equiv ar_2(\mod q)\\
&(a,q)=1\Rightarrow r_1\equiv r_2(\mod q)\\
&\Rightarrow r_1=r_2
\end{aligned}$$

در نتیجه برای هر $t\in[0,\frac{q-1}{q}]$ حداکثر چهار عدد صحیح $r\in[1,q]$ وجود دارد به طوری که $\{\alpha(hq+r)\}\in[t,t+\frac{1}{q}]$. توجه کنید که

$$||\alpha(hq+r)||\in[t,t+\frac{1}{q}]\iff\{\alpha(hq+r)\}\in[t,t+\frac{1}{q}]$$

$$\text{یا } 1-\{\alpha(hq+r)\}\in[t,t+\frac{1}{q}]$$

همچنین داریم

$$\begin{aligned}
&1-\{\alpha(hq+r)\}\in[t,t+\frac{1}{q}]\\
&\Rightarrow\{\alpha(hq+r)\}\in[t',t'+\frac{1}{q}],0\leq t'=1-\frac{1}{q}-t\leq 1-\frac{1}{q}
\end{aligned}$$

این نتیجه می‌دهد برای هر $t\in[0,\frac{q-1}{q}]$ حداکثر هشت عدد صحیح $r\in[1,q]$ وجود دارد که

$$||\alpha(hq+r)||\in J(s):=[\frac{s}{q},\frac{s+1}{q}]$$

اکنون به اثبات حکم می‌پردازیم. اگر $||\alpha(hq+r)||\in J(0)$ از نابرابری $\min\{V,||\alpha(hq+r)||^{-1}\}\leq V$ و اگر داشته باشیم $||\alpha(hq+r)||\in J(s)$ که $s\geq 1$ آن‌گاه از نابرابری زیر استفاده می‌کنیم

$$\min\{V,||\alpha(hq+r)||^{-1}\}\leq||\alpha(hq+r)||\leq\frac{q}{s}$$

با توجه به اینکه به ازای هر r وجود دارد $s<\frac{q}{2}$ که $||\alpha(hq+r)||\in J(s)$، داریم

$$\begin{aligned}
\sum_{1\leq s\leq q}\min\{V,||\alpha(hq+r)||^{-1}\}&\leq 8V+8\sum_{1\leq s<\frac{q}{2}}\frac{q}{s}\\
&\ll V+q\log q
\end{aligned}$$

اثبات کامل شد. □

اثبات (i): k را می‌توانیم به شکل زیر بنویسیم

$$k = hq + r, 1 \le r \le q, 0 \le h < \frac{U}{q}$$

در نتیجه داریم

$$\begin{aligned} S &:= \sum_{1\le k\le U} \min\{\frac{n}{k}, ||\alpha k||^{-1}\} \\ &\le \sum_{0\le h<\frac{U}{q}}\sum_{1\le r\le q} \min\{\frac{n}{hq+r}, ||\alpha(hq+r)||^{-1}\} \end{aligned}$$

اگر $h = 0$ و $1 \le r \le \frac{q}{2}$ آن‌گاه لم ۱۹ نتیجه می‌دهد

$$\sum_{1\le r\le \frac{q}{2}} \min\{\frac{n}{r}, ||\alpha r||^{-1}\} \le \sum_{1\le r\le \frac{q}{2}} ||\alpha r||^{-1} << q\log q$$

برای بقیه جملات داریم $\frac{1}{hq+r} < \frac{2}{(h+1)q}$. زیرا

$$h \ge 1 \Rightarrow hq + r > hq \ge \frac{(h+1)q}{2}$$

$$h = 0, \frac{q}{2} < r \le q \Rightarrow hq + r = r > \frac{q}{2} = \frac{(h+1)q}{2}$$

در نتیجه داریم

$$S \ll q\log q + \sum_{0\le h<\frac{U}{q}}\sum_{1\le r\le q} \min\{\frac{n}{(h+1)q}, ||\alpha(hq+r)||^{-1}\}$$

با توجه به اینکه $\frac{U}{q} + 1 \le U + q \le 2\max\{q, U\} \le 2qU$ و با قرار دادن $V = \frac{n}{(h+1)q}$ در لم ۲۰ به دست می‌آوریم

$$\begin{aligned} S &\ll q\log q + \sum_{0\le h<\frac{U}{q}}\sum_{1\le r\le q} \min\{\frac{n}{(h+1)q}, ||\alpha(hq+r)||^{-1}\} \\ &\ll q\log q + \sum_{0\le h<\frac{U}{q}} (\frac{n}{(h+1)q} + q\log q) \\ &\ll q\log q + \frac{n}{q}\sum_{0\le h<\frac{U}{q}} \frac{1}{h+1} + (\frac{U}{q}+1)q\log q \\ &\ll q\log q + \frac{n}{q}\log(\frac{U}{q}+1) + U\log q + q\log q \\ &\ll (\frac{n}{q} + U + q)\log 2qU \end{aligned}$$

حکم اثبات شد.

(ii)

$\sum_{n\le x} d(n)^2 \ll x(\log x)^3$. برای اثبات به یک لم ساده نیاز داریم.

لم ۲۱. $D(x) := \sum_{n\le x} d(n) = x\log x + (2\gamma - 1)x + O(\sqrt{x})$.

اثبات. توجه کنید که $d(n) = \sum_{d|n} 1$ نشان دهنده‌ی تعداد نقاط شبکه‌ای روی سهمی $uv = n$ است که در ربع اول صفحه مختصات قرار دارند. در نتیجه $D(x)$ برابر است با تعداد نقاط شبکه‌ای از ربع اول است روی یا زیر سهمی $uv = x$ قرار دارند. در واقع برابر است با تعداد نقاط با مختصات صحیح مثبت (u, v) به طوری که $1 \le u \le x$ و $1 \le v \le \frac{x}{u}$. این مجموعه از نقاط را می‌توانیم به سه مجموعه‌ی مجزا افراز کنیم:

$$\{1 \le u \le \sqrt{x}, 1 \le v \le \sqrt{x}\}$$

$$\{1 \le u \le \sqrt{x}, \sqrt{x} < v \le \frac{x}{u}\}$$

$$\{\sqrt{x} < u \le x, 1 \le v \le \frac{x}{u}\}$$

همچنین توجه کنید که داریم:

$$\{\sqrt{x} < u \le x, 1 \le v \le \frac{x}{u}\} = \{1 \le v \le \sqrt{x}, \sqrt{x} < u \le \frac{x}{v}\}$$

در نتیجه داریم:

$$\begin{aligned} D(x) &= \lfloor\sqrt{x}\rfloor^2 + \sum_{1\le u\le\sqrt{x}} (\lfloor\frac{x}{u}\rfloor - \lfloor\sqrt{x}\rfloor) \\ &\quad + \sum_{1\le v\le\sqrt{x}} (\lfloor\frac{x}{v}\rfloor - \lfloor\sqrt{x}\rfloor) \\ &= \lfloor\sqrt{x}\rfloor^2 + 2\sum_{1\le u\le\sqrt{x}} (\lfloor\frac{x}{u}\rfloor - \lfloor\sqrt{x}\rfloor) \\ &= 2\sum_{1\le u\le\sqrt{x}} \lfloor\frac{x}{u}\rfloor - \lfloor\sqrt{x}\rfloor^2 \\ &= 2\sum_{1\le u\le\sqrt{x}} (\frac{x}{u} - \{\frac{x}{u}\}) - (\sqrt{x} - \{\sqrt{x}\})^2 \\ &= 2x\sum_{1\le u\le\sqrt{x}} \frac{1}{u} - 2\sum_{1\le u\le\sqrt{x}} \{\frac{x}{u}\} - x + O(\sqrt{x}) \\ &= 2x(\log\sqrt{x} + \gamma + O(\frac{1}{\sqrt{x}})) - x + O(\sqrt{x}) \\ &= x\log x + (2\gamma - 1)x + O(\sqrt{x}) \end{aligned}$$

که در آن γ ثابتی است با این ویژگی که

$$\sum_{1\le n\le x} \frac{1}{n} = \log x + \gamma + O(\frac{1}{x})$$

اثبات به پایان رسید. □

اثبات (ii): ابتدا توجه کنید که برای هر $a, b \in \mathbb{N}$ داریم $d(ab) \le d(a)d(b)$ (این حکم را می‌توان به راحتی با نوشتن a و b به صورت حاصل‌ضرب توان‌های اعداد اول اثبات کرد و ما از نوشتن اثبات

خودداری می‌کنیم). با توجه به این نکته داریم

$$\begin{aligned}
\sum_{n\le x} d(n)^2 &= \sum_{n\le x} d(n)\sum_{n=ab} 1 = \sum_{ab\le x} d(ab)\\
&\le \sum_{ab\le x} d(a)d(b) = \sum_{a\le x} d(a)\sum_{b\le \frac{x}{a}} d(b)\\
&\overset{\text{استفاده از لم ۲۱}}{=} \sum_{a\le x} d(a)\big((\frac{x}{a})\log(\frac{x}{a}) + O(\frac{x}{a})\big)\\
&\le x\log x \sum_{a\le x}\frac{d(a)}{a} + O(x\sum_{a\le x}\frac{d(a)}{a})\\
&\ll x(\log x)^3
\end{aligned}$$

حکم ثابت شد.

(iii)

قضیه‌ی دیریکله: فرض کنید Q و α اعداد حقیقی باشند و $Q\ge 1$.
در این صورت اعداد صحیح a,q با شرایط زیر موجودند

$$1\le q\le Q, (a,q)=1, |\alpha-\frac{a}{q}|<\frac{1}{qQ}$$

اثبات (iii): قرار می‌دهیم $N=\lfloor Q\rfloor$. فرض کنید برای عددی طبیعی مانند q با $q\le Q$ داشته باشیم $\{q\alpha\}\in[0,\frac{1}{N+1})$. اگر $a=\lfloor q\alpha\rfloor$، آن‌گاه

$$0\le\{q\alpha\}=q\alpha-\lfloor q\alpha\rfloor=q\alpha-a<\frac{1}{N+1}$$

$$|\alpha-\frac{a}{q}|<\frac{1}{q(N+1)}<\frac{1}{qQ}$$

هم‌چنین اگر برای $q\le Q$ای داشته باشیم $\{q\alpha\}\in[\frac{N}{N+1},1)$. اگر $a=\lfloor q\alpha\rfloor+1$، آن‌گاه

$$\frac{N}{N+1}\le\{q\alpha\}=q\alpha-a+1<1$$

$$\Rightarrow |q\alpha-a|\le\frac{1}{N+1}\Rightarrow|\alpha-\frac{a}{q}|\le\frac{1}{q(N+1)}<\frac{1}{qQ}$$

پس در این حالات حکم درست است. اکنون اگر برای هر $q\in\{1,2,\dots,N\}$ داشته باشیم $\{q\alpha\}\in[\frac{1}{N+1},\frac{N}{N+1}]$، آن‌گاه N عدد حقیقی $\{q\alpha\}$ در $N-1$ بازه‌ی $[\frac{i}{N+1},\frac{i+1}{N+1})$ برای $i=1,2,\dots,N-1$ قرار دارند و بنابر اصل لانه‌کبوتری $i\in\{1,\dots,N\}$ و $q_1,q_2\in\{1,\dots,N\}$ موجود است به طوری که

$$q_1<q_2, \{q_1\alpha\},\{q_2\alpha\}\in[\frac{i}{N+1},\frac{i+1}{N+1})$$

اگر $q=q_2-q_1\in[1,N-1]$ و $a=\lfloor q_2\alpha\rfloor-\lfloor q_1\alpha\rfloor$، آن‌گاه

$$\begin{aligned}
|q\alpha-a| &= |(q_2\alpha-\lfloor q_2\alpha\rfloor)-(q_1\alpha-\lfloor q_1\alpha\rfloor)|\\
&= |\{q_2\alpha\}-\{q_1\alpha\}|<\frac{1}{N+1}<\frac{1}{Q}\\
&\Rightarrow |\alpha-\frac{a}{q}|<\frac{1}{qQ}
\end{aligned}$$

اثبات حکم کامل شد.

مراجع

[1] Steven J. Miller, Ramin Takloo-Bighash - The Circle Method

[2] R. C. Vaughan - The Hardy-Littlewood Method (Second Edition), Cambridge University Press

[3] Ian N. Petro - Vinogradov's Three Primes Theorem

[4] Melvyn B. Nathanson - Additive Number Theory (The Classical Bases) , Springer

[5] I. M. Vinogradov - The Method of Trigonometrical Sums in the Theory of Numbers