Адитивни задачи в теорията на числата

Д. И. Толев

Записки по едноименния изборен курс, четен от автора
във ФМИ при СУ „Св. Климент Охридски“
през летния семестър на учебната
2008/2009 г.

София, октомври 2009 г.

Съдържание

1 Увод **3**

1.1 Означения . . . 3

1.2 Исторически сведения . . . 4

2 Проблемите на Голдбах **5**

2.1 Формулировка на теоремите . . . 5

2.2 Доказателство на Теорема 2 . . . 7

2.2.1 Начало на доказателството . . . 7

2.2.2 Оценяване на $\mathcal{E}_1$. . . . 9

2.2.3 Оценяване на $\mathcal{E}_2$. . . . 19

2.2.4 Край на доказателството. . . . 33

2.3 Тернарният проблем на Голдбах. . . . 33

3 Проблем на Варинг **40**

3.1 Увод и формулировка на теоремата . . . 40

3.2 Доказателство на Теорема 10. . . . 40

3.2.1 Начало на доказателството. . . . 40

3.2.2 Оценка на I''. . . . 41

3.2.3 Асимптотична формула за I'. . . . 51

3.2.4 Изследване на особения ред $\mathfrak{S}_{k,n}(N)$. . . . 60

4 Допълнение **70**

4.1 Функцията $e(\alpha)$. . . . 70

4.2 Рационални приближения на реални числа. . . . 70

4.3 Някои известни неравенства . . . 70

4.4 Леми от математическия анализ . . . 71

4.5 Аритметични функции . . . 72

4.5.1 Някои основни аритметични функции . . . 72

4.6 Системи от остатъци и сравнения . . . 74

4.7 Показатели и примитивни корени . . . 75

4.8 Разпределение на простите числа . . . 75

1 Увод

1.1 Означения

Както обикновено $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$ и $\mathbb{C}$ са множествата на естествените, целите, реалните и комплексните числа. С буквите x, y и с гръцките букви ще означаваме реални числа, като ε ще бъде произволно малко положително число, което не е едно и също в различни формули. С малките латински букви ще означаваме цели или естествени числа, но буквата p ще е запазена за простите числа.

Ще използуваме обичайните означения от теорията на числата. В частност, $a \mid b$ и $a \nmid b$ означава, че a дели b, съответно, че a не дели b. Както обикновено, $a \equiv b \pmod q$ означава, че a е сравнимо с b по модул q. Най-големият общ делител на числата a и b ще бележим с (a, b), а тяхното най-малко общо кратно с $[a, b]$. (Понякога по същия начин бележим отворен, съответно затворен, интервал с краища a и b, но във всеки конкретен случай смисълът става ясен от контекста.) Ако $\alpha \in \mathbb{R}$, то с $[\alpha]$, $\{\alpha\}$ и $||\alpha||$ ще означаваме цялата част на α, дробната част на α и разстоянието от α до най-близкото цяло число. $\log \alpha$ е натурален логаритъм от α. Също така, за краткост бележим $e(\alpha) = e^{2\pi i\alpha} = \cos(2\pi\alpha) + i\sin(2\pi\alpha)$.

Ще употребяваме означенията на Ландау $X = O(Y)$ и съответно на Виноградов $X \ll Y$, като и двете са съкратен запис на твърдението „Съществува константа $c > 0$ такава, че $|X| \leq cY$“. Ако c зависи от някои други константи, например γ, δ то понякога ще отразяваме този факт, чрез означенията $X = O_{\gamma,\delta}(Y)$, съответно $X \ll_{\gamma,\delta} Y$. При $X \ll Y$ и $Y \ll X$ ще пишем за по-кратко $X \asymp Y$.

Ще използуваме общоприетите означения за основните аритметични функции (виж допълнението за техните определения и основни свойства), а именно
$\mu(n)$ — функция на Мьобиус;
$\varphi(n)$ — функция на Ойлер;
$\tau(n)$ — брой на делителите на естественото число q;
$\Lambda(n)$ — функция на Манголд.
$c_n(q)$ — сума на Рамануджан.

Както обикновено $\sum_{k \leq X}$ и $\sum_{p \leq x}$ са суми по всички естествени, съответно прости числа, ненадминаващи X, $\sum_{d|n}$ е сума по положителните делители на n, $\prod_{p|n}$ е произведение по простите делители на n, а $\prod_p$ е произведение по всички прости числа.

Със знака $\Box$ ще бележим края на доказателство на някакво твърдение, или отсъствие на доказателство.

1.2 Исторически сведения

През 1742 г. Голдбах, в писмо до Ойлер, е изказал две знаменити хипотези.

Бинарна хипотеза: Всяко четно число по-голямо от 2 се представя като сума на две прости числа.

Тернарна хипотеза: Всяко нечетно число по-голямо от 5 се представя като сума на три прости числа.

През 1937 г. Виноградов доказва тернарната хипотеза за достатъчно големи нечетни числа. Бинарната хипотеза в насточщия момент не е доказана, но са установени голям брой резултати, които в един или друг аспект са приближения към нея.

През 1770 г. Лагранж е доказал, че всяко естествено число се представя като сума на четири квадрата на цели числа. През същата година Варинг е изказал хипотезата, известна като

Проблем на Варинг: Да се докаже, че за всяко цяло $n \geq 2$ може да се намери $k_0 = k_0(n)$ такова, че всяко естествено число може да се представи като сума на не повече от k_0 на брой n-ти степени на естествени числа.

През 18-ти и 19-ти век са били доказани голям брой частни случаи на това твърдение, но пълно доказателство е намерено едва през 1909 г. от Хилберт. Методът на Хилберт е много сложен и освен това величината $k_0(n)$ е изключително бързорастяща функция на n.

В периода 1920 – 1930, в поредица от статии, Харди и Литлууд разработват така наречения *кръгов метод* и с негова помощ намират значително по-просто решение на проблема на Варинг. При това, методът на Харди и Литлууд позволява величината $k_0(n)$, определена по-горе, да бъде значително по-бавно растяща функция на n.

Впоследствие кръговият метод е усъвършенстван от Виноградов, Хуа и други математици, а напредъкът при изучаването на проблема на Варинг и сродни въпроси е значителен. Тук ще отбележим, че предмет на изследванията е не само разрешимостта на уравнението

$$x_1^n + \cdots + x_k^n = N$$

в естествени числа $x_1, \ldots, x_k$, но също и информация за броя на неговите решения.

В настоящите записки ще формулираме и докажем някои класически теореми. В Глава 2 ще се занимаем с резултати, отнасящи се до проблемите на Голдбах, а в Глава 3 — с проблема на Варинг. Ще използваме наготово добре познати понятия и резултати от елементарната теория на числата. За улеснение на читателя, съответните определения и леми са формулирани в Глава 4. Единственият по-дълбок резултат от теорията на числата, който ще използваме, но няма да докажем, е класическата теорема на Зигел за разпределението на простите числа в аритметични прогресии (виж Лема 54 от Глава 4).

Изложението в записките е близко до това в книгите на Карацуба [2] и Вон [6], но доказателствата и изчисленията, които привеждаме, са доста по-подробни. Ще препоръчаме на читателя също известните уводни книги по теория на числата на Виноградов [1], Чандрасекхаран [4], Харди и Райт [5] и книгата по теория на функциите на Титчмарш [3].

2 Проблемите на Голдбах

2.1 Формулировка на теоремите

За всяко $N \in \mathbb{N}$ означаваме

$$R^{(3)}(N) = \sum_{p_1+p_2+p_3=N} (\log p_1)(\log p_2)(\log p_3) \tag{1}$$

където сумирането се извършва по всички тройки прости числа, за които е изпълнено $p_1 + p_2 + p_3 = N$. Виноградов е доказал следната

Теорема 1. *В сила е следната асимптотична формула:*

$$R^{(3)}(N) = \frac{1}{2} N^2 \mathfrak{S}^{(3)}(N) + O_A\left(\frac{N^2}{(\log N)^A}\right), \tag{2}$$

където $A > 0$ е произволно голяма константа и

$$\mathfrak{S}^{(3)}(N) = \prod_{p \nmid n} \left(1 + \frac{1}{(p-1)^3}\right) \prod_{p \mid n} \left(1 - \frac{1}{(p-1)^2}\right). \tag{3}$$

Лесно се вижда, че ако $2 \nmid N$, то

$$0 < c_1 < \mathfrak{S}^{(3)}(N) < c_2,$$

където c_1, c_2 са константи. Тогава ако N е достатъчно голямо нечетно число, то $R^{(3)}(N) > 0$, т.е. следва верността на тернарната хипотеза.

Както споменахме в Увода, бинарната хипотеза на Голдбах все още не е доказана, но са получени голям брой теореми, които са приближения към нея. Резултат от такъв тип е Теорема 2, формулирана по-долу. В настоящите записки тя ще бъде подробно доказана и ще бъдат получени нейни следствия. В частност, ще видим, че като се използва Теорема 2, може сравнително лесно да се докаже Теорема 1. (Това е извършено в § 2.3.)

За всяко $n \in \mathbb{N}$ определяме

$$R(n) = \sum_{p_1+p_2=n} (\log p_1)(\log p_2). \tag{4}$$

Предполага се, че е в сила асимптотичната формула

$$R(n) = n\mathfrak{S}(n) + O_A\left(\frac{n}{(\log n)^A}\right), \tag{5}$$

където $A > 0$ е произволно голяма константа и

$$\mathfrak{S}(n) = \prod_{p \nmid n} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{p \mid n} \left(1 + \frac{1}{p-1}\right). \tag{6}$$

Нека разгледаме $\mathfrak{S}(n)$. Ако $2 \nmid n$, то $\mathfrak{S}(n) = 0$ тъй като първото произведение съдържа множителя $1 - \frac{1}{(2-1)^2} = 0$. (Да отбележим, че при $2 \nmid n$ от условието $p_1 + p_2 = n$ следва, че едно от простите числа е равно на 2, тъй че ще имаме $R(n) = O(\log n)$. Тогава формулата (5) е вярна, но е тривиална.)

Нека $2 \mid n$. Тогава произведенията в (6) не съдържат нулев множител и ще имаме

$$\mathfrak{S}(n) \geq \prod_{k=2}^{\infty} \left(1 - \frac{1}{k^2}\right) > 0. \tag{7}$$

Величината $\mathfrak{S}(n)$ се оценява лесно и отгоре. Като използваме (6) и вземем предвид Леми 42 и 43, намираме

$$\mathfrak{S}(n) \leq \prod_{p \mid n} \left(1 + \frac{1}{p-1}\right) = \prod_{p \mid n} \left(1 - \frac{1}{p}\right)^{-1} = \frac{n}{\varphi(n)} \ll \log\log(10n). \tag{8}$$

От неравенството (7) и от асимптотичната формула (5) следва, че $R(n) > 0$ за достатъчно големи четни n, или че всяко достатъчно голямо четно число се представя като сума на две прости числа. Както вече споменахме, обаче, до настоящия момент формула (5) не е доказана.

При $N \in \mathbb{N}$ означаваме

$$\mathcal{E}(N) = \sum_{n \leq N} |R(n) - n\mathfrak{S}(n)|^2. \tag{9}$$

В сила е следната

Теорема 2. *За всяка константа $A > 0$ е в сила неравенството*

$$\mathcal{E}(N) \ll_A \frac{N^3}{(\log N)^A}. \tag{10}$$

Теорема 2 е доказана през 1938 г., с помощта на метода на Виноградов, независимо от Ван-дер-Корпут, Естерман и Чудаков.

И така, въпреки че не е известно дали асимптотичната формула (5) е изпълнена за конкретна стойност на n, то от оценката (10) следва, че остатъчният член в (5) е „малък“ в средноквадратичен смисъл. Този факт е интересен сам по себе си, но от него се получават също и други интересни резултати. С един от тях — решение на тернарния проблем на Голдбах за достатъчно големи нечетни числа — ще се запознаем още сега.

Следствие 3. *Всяко достатъчно голямо нечетно число се преставя като сума на три прости числа.*

Доказателство. Да допуснем, че N е нечетно число, което не се представя като сума на три прости числа. Разглеждаме сумата

$$S = \sum_{2<p\le N/2} \left| R(N-p) - (N-p)\mathfrak{S}(N-p) \right|. \tag{11}$$

Според нашето допускане ще имаме $R(N-p) = 0$ за всяко просто p, удовлетворяващо $2 < p \le N/2$. Тогава от (11) следва

$$S = \sum_{2<p\le N/2} (N-p)\mathfrak{S}(N-p).$$

Но от (7) и от теоремата на Чебишев (Лема 52) получаваме

$$S \gg N\left(\pi(N/2) - 1\right) \gg \frac{N^2}{\log N}. \tag{12}$$

От друга страна, като използваме (9), (11) и неравенството на Коши (Лема 30), получаваме

$$S \le \sum_{n\le N} |R(n) - n\mathfrak{S}(n)| \le \sqrt{N\,\mathcal{E}(N)}$$

и, като приложим Теорема 2 при $A = 4$, намираме

$$S \ll \frac{N^2}{(\log N)^2}. \tag{13}$$

Неравенствата (12) и (13) са несъвместими ако N е достатъчно голямо. С това Следствие 3 е доказано. □

От Теорема 2 като следствие може да се получи и не само разрешимостта на тернарното уравнение на Голдбах, но също и информацията за броя на решенията му, дадена в Теорема 1. Както споменахме, това е извършено в § 2.3.

2.2 Доказателство на Теорема 2

2.2.1 Начало на доказателството

Нека $N \in \mathbb{R}$ е достатъчно голямо и нека $n \in \mathbb{N}$, като $n \le N$. Като използваме Лема 27 (свойства (4), (5)), преобразуваме величната $R(n)$, определена чрез (4), във вида

$$
\begin{aligned}
R(n) &= \sum_{\substack{p_1,p_2\le N\\ p_1+p_2=n}} (\log p_1)(\log p_2)\\
&= \sum_{p_1,p_2\le N} (\log p_1)(\log p_2) \int\limits_0^1 e(\alpha(p_1+p_2-n))\,d\alpha\\
&= \int\limits_0^1 \sum_{p_1,p_2\le N} (\log p_1)(\log p_2)\, e(\alpha p_1)\, e(\alpha p_2)\, e(-\alpha n)\,d\alpha\\
&= \int\limits_0^1 S^2(\alpha)\, e(-\alpha n)\,d\alpha, \qquad (14)
\end{aligned}
$$

където

$$
S(\alpha) = S_N(\alpha) = \sum_{p\le N} (\log p)\, e(\alpha p). \qquad (15)
$$

За да получим полезна информация за $R(n)$ е необходимо да изследваме сумата $S(\alpha)$. Първо ще споменем, че за всяко $\alpha \in \mathbb{R}$ е вярна следната тривиална оценка, безираща се на неравенството на триъгълника (Лема 29) и на Теоремата на Чебишев (Лема 52):

$$
|S(\alpha)| \le \sum_{p\le N} \log p = \theta(N) \ll N. \qquad (16)
$$

Оказва се, че ако α е „близко“ до рационална дроб с „малък“ знаменател, то за $S(\alpha)$ може да бъде получена асимптотична формула. Ако пък α не притежава горното свойство, то ще видим, че за модула на сумата $S(\alpha)$ може да бъде получена оценка по-точна отколкото в (16).

За да дадем количествен израз на горните съображения, въвеждаме параметрите

$$
Q = (\log N)^{A_1}, \qquad \tau = \frac{N}{(\log N)^{A_2}}, \qquad (17)
$$

където $A_1 > 0$, $A_2 > 0$ са константи, които ще изрзим по подходящ начин чрез константата A в края на доказателството на теоремата.

Определяме множеството от *големите дъги*

$$
\mathfrak{M} = \bigcup_{q\le Q} \bigcup_{\substack{a=0\\ (a,q)=1}}^{q-1} \left[\frac{a}{q} - \frac{1}{q\tau}, \frac{a}{q} + \frac{1}{q\tau}\right]. \qquad (18)
$$

Това е множество от числа, които са на разстояние от дроб със знаменател $q \le Q$ не по-голямо от $(q\tau)^{-1}$. Очевидно

$$
\mathfrak{M} \subset \left[-\frac{1}{\tau}, 1 - \frac{1}{\tau}\right]. \qquad (19)
$$

Определяме и множеството от *малките дъги* чрез

$$\mathfrak{m} = \left[-\frac{1}{\tau}, 1 - \frac{1}{\tau}\right] \setminus \mathfrak{M}. \tag{20}$$

Ще отбележим, че множествата $\mathfrak{M}$ и $\mathfrak{m}$ са всъщност крайни обединения от интервали, но термините „големи дъги“ и „малки дъги“ се използват по традиция.

Като използваме свойство 1 от Лема 27 виждаме, че функцията $S(\alpha)$, определена чрез (15), е периодична с период 1. Тогава същото свойство притежава и подинтегралната функция в (14), следователно

$$R(n) = \int\limits_{-\frac{1}{\tau}}^{1-\frac{1}{\tau}} S^2(\alpha)\, e(-\alpha n)\, d\alpha.$$

От горното равенство и от (19), (20) получаваме

$$R(n) = R_1(n) + R_2(n), \tag{21}$$

където

$$R_1(n) = \int\limits_{\mathfrak{M}} S^2(\alpha)\, e(-\alpha n)\, d\alpha, \qquad R_2(n) = \int\limits_{\mathfrak{m}} S^2(\alpha)\, e(-\alpha n)\, d\alpha. \tag{22}$$

Като използваме (9) и (21) намираме

$$\mathcal{E}(N) \ll \mathcal{E}_1 + \mathcal{E}_2, \tag{23}$$

където

$$\mathcal{E}_1 = \sum_{n \le N} |R_1(n) - n\mathfrak{S}(n)|^2, \qquad \mathcal{E}_2 = \sum_{n \le N} |R_2(n)|^2. \tag{24}$$

Предстои ни да оценим сумата $\mathcal{E}_1$, след което ще се занимаем и със сумата $\mathcal{E}_2$.

2.2.2 Оценяване на $\mathcal{E}_1$.

Начало на изследването. Първо да отбележим, че интервалите, съставящи множеството $\mathfrak{M}$, определено чрез (18), два по два не се пресичат. Наистина, да вземем два различни такива интервала с центрове, съответно a/q и a'/q'. Разстоянието между тези две точки е равно на

$$\left|\frac{a}{q} - \frac{a'}{q'}\right| = \frac{|aq' - a'q|}{qq'} \ge \frac{1}{qq'}.$$

Тук използвахме, че $aq' - a'q \ne 0$. Наистина, ако $aq' = a'q$, то като вземем предвид, че $(a, q) = (a', q') = 1$ ще получим $a = a'$, $q = q'$. Последното не е възможно, тъй като $a/q \ne a'/q'$.

От друга страна, сумата от радиусите на нашите два интервала е равна на $1/(q\tau) + 1/(q'\tau)$. Като използваме условията $q \leq Q$, $q' \leq Q$ и определенията на Q и τ дадени в (17), виждаме, че при достатъчно големи N е изпълнено

$$\frac{1}{qq'} > \frac{1}{q\tau} + \frac{1}{q'\tau}.$$

Следователно нашите два интервала не могат да се пресичат.

Тогава от (18) и (22) следва

$$R_1(n) = \sum_{q \leq Q} \sum_{\substack{a=0 \\ (a,q)=1}}^{q-1} \int_{\frac{a}{q}-\frac{1}{q\tau}}^{\frac{a}{q}+\frac{1}{q\tau}} S^2(\alpha)\, e(-\alpha n)\, d\alpha$$

и след смяна на променливата в горния интеграл получаваме

$$R_1(n) = \sum_{q \leq Q} \sum_{\substack{a=0 \\ (a,q)=1}}^{q-1} H_{a,q}(n), \tag{25}$$

където

$$H_{a,q}(n) = \int_{-1/(q\tau)}^{1/(q\tau)} S^2\left(\frac{a}{q} + \beta\right) e\left(-\left(\frac{a}{q} + \beta\right) n\right) d\beta. \tag{26}$$

Асимптотична формула за експоненциалната сума. За да продължим понататък, трябва да изследваме сумата $S\left(\frac{a}{q} + \beta\right)$ при условие, че

$$q \leq Q, \qquad (a,q) = 1, \qquad |\beta| \leq \frac{1}{q\tau}. \tag{27}$$

Изпълнена е следната

Лема 4. *Ако са налице условията (27), то е в сила асимптотичната формула*

$$S\left(\frac{a}{q} + \beta\right) = \frac{\mu(q)}{\varphi(q)} M(\beta) + O\left(N e^{-c\sqrt{\log N}}\right), \tag{28}$$

където

$$M(\beta) = \sum_{m \leq N} e(\beta m), \tag{29}$$

$c > 0$ е константа, а $\mu(q)$ и $\varphi(q)$ са съответно функцията на Мьобиус на и функцията на Ойлер.

Доказателство. Първо, като използваме (15) и Лема 52, оценяваме тривиално приноса към сумата $S(a/q+\beta)$, идващ от малките прости числа. След това разделяме сумата на части съобразно остатъка на p по модул q. Получаваме

$$S\left(\frac{a}{q}+\beta\right)=\sum_{\sqrt{N}<p\le N}(\log p)\,e\left(\left(\frac{a}{q}+\beta\right)p\right)+O\left(\sqrt{N}\right)$$

$$=\sum_{m=0}^{q-1}\sum_{\substack{\sqrt{N}<p\le N\\ p\equiv m \pmod q}}(\log p)\,e\left(\left(\frac{a}{q}+\beta\right)p\right)+O\left(\sqrt{N}\right).$$

Като използваме горната формула и свойства (1) и (4) на Лема 27, намираме

$$S\left(\frac{a}{q}+\beta\right)=\sum_{m=0}^{q-1}e\left(\frac{am}{q}\right)\,Z_m+O\left(\sqrt{N}\right), \tag{30}$$

където

$$Z_m=\sum_{\substack{\sqrt{N}<p\le N\\ p\equiv m \pmod q}}(\log p)\,e(\beta p). \tag{31}$$

В сумата по m в (30) всъщност участват само събираеми, за които $(m,q)=1$. Наистина, ако $(m,q)=k>1$, то от условието $p\equiv m \pmod q$ ще следва $k\mid p$ и, тъй като p е просто число, $k=p>\sqrt{N}$. От друга страна $k\le q\le Q$ и като използваме определението на Q, дадено в (17), виждаме, че при достатъчно голямо N се получава противоречие.

И така, намираме

$$S\left(\frac{a}{q}+\beta\right)=\sum_{\substack{m=0\\ (m,q)=1}}^{q-1}e\left(\frac{am}{q}\right)\,Z_m+O\left(\sqrt{N}\right). \tag{32}$$

За да получим асимптотична формула за Z_m ще използваме теормата на Зигел (Лема 54). Първо прилагаме преобразованието на Абел (Лема 31) и записваме Z_m във вида

$$Z_m=-\int_{\sqrt{N}}^{N}\left(\sum_{\substack{\sqrt{N}<p\le t\\ p\equiv m \pmod q}}(\log p)\right)\frac{d}{dt}\left(e(\beta t)\right)\,dt+e(\beta N)\sum_{\substack{\sqrt{N}<p\le N\\ p\equiv m \pmod q}}(\log p). \tag{33}$$

Ако $\sqrt{N}\le t\le N$ имаме $\frac{1}{2}\log N\le\log t\le\log N$, тъй че при $q\le Q=(\log N)^{A_1}$ условието за горната граница на модула в теоремата на Зигел ще е изпълнено. Тогава при $\sqrt{N} \le t \le N$ имаме

$$\sum_{\substack{\sqrt{N}<p\le t \\ p\equiv m \pmod q}} (\log p) = \sum_{\substack{p\le t \\ p\equiv m \pmod q}} (\log p) + O\left(\sqrt{N}\right)$$

$$= \frac{t}{\varphi(q)} + O\left(te^{-c\sqrt{\log t}}\right) + O\left(\sqrt{N}\right)$$

$$= \frac{t}{\varphi(q)} + O\left(Ne^{-c'\sqrt{\log N}}\right). \qquad (34)$$

В горната формула $c' = c/\sqrt{2}$ също е положителна константа, която наново ще означим с c. (По подобен начин ще действаме и по-нататък, тъй че при нас c е някаква положителна константа, която не е една и съща в различни формули.)

Заместваме израза от (34) в (33) и получаваме

$$Z_m = -\int_{\sqrt{N}}^{N} \left(\frac{t}{\varphi(q)} + O\left(Ne^{-c\sqrt{\log N}}\right)\right) \frac{d}{dt}\left(e(\beta t)\right)\, dt$$

$$+ e(\beta N)\left(\frac{N}{\varphi(q)} + O\left(Ne^{-c\sqrt{\log N}}\right)\right)$$

$$= \frac{1}{\varphi(q)}\left(-\int_{\sqrt{N}}^{N} t\,\frac{d}{dt}\left(e(\beta t)\right)\, dt + Ne(\beta N)\right)$$

$$+ O\left(Ne^{-c\sqrt{\log N}}\left(1 + \int_{0}^{N}\left|\frac{d}{dt}\left(e(\beta t)\right)\right| dt\right)\right). \qquad (35)$$

За да оценим интеграла, намиращ се в остатъчния член в (35), използваме (17) и (27) и получаваме

$$\int_{0}^{N}\left|\frac{d}{dt}\left(e(\beta t)\right)\right| dt = \int_{0}^{N} |2\pi i\beta\, e(\beta t)|\, dt \ll |\beta| N \ll \frac{N}{q\tau} \ll (\log N)^{A_2}. \qquad (36)$$

Тогава остатъчният член от (35) е

$$\ll Ne^{-c\sqrt{\log N}}(\log N)^{A_2} \ll Ne^{-c'\sqrt{\log N}},$$

където $c' \in (0, c)$ е нова константа, която пак ще означаваме с c.

Да разгледаме главния член в предпоследния ред на (35). Като интегрираме по части, получаваме, че той е равен на

$$\frac{1}{\varphi(q)}\left(-Ne(\beta N)+\sqrt{N}e(\beta\sqrt{N})+\int\limits_{\sqrt{N}}^{N} e(\beta t)\,dt+Ne(\beta N)\right)$$
$$=\frac{1}{\varphi(q)}\int\limits_{0}^{N} e(\beta t)\,dt+O\left(\sqrt{N}\right).$$

Следователно от (35) и от горните оценки следва

$$Z_m=\frac{1}{\varphi(q)}\int\limits_{0}^{N} e(\beta t)\,dt+O\left(Ne^{-c\sqrt{\log N}}\right). \tag{37}$$

Сега ще проверим, че интегралът от (37) се различава малко от сумата $M(\beta)$, определена чрез (29). Наистина, като използваме сумационната формула на Ойлер (Лема 32), намираме

$$M(\beta)=\sum_{0<m\le N} e(\beta m)$$

$$=\int\limits_{0}^{N} e(\beta t)\,dt+\rho(N)e(\beta N)-\rho(0)e(0)-\int\limits_{0}^{N}\rho(t)\frac{d}{dt}\left(e(\beta t)\right)\,dt$$

$$=\int\limits_{0}^{N} e(\beta t)\,dt+O(1)+O\left(\int\limits_{0}^{N}\left|\frac{d}{dt}\left(e(\beta t)\right)\right|\,dt.\right)$$

Сега се възползваме от (36) и получаваме

$$M(\beta)=\int\limits_{0}^{N} e(\beta t)\,dt+O\left((\log N)^{A_2}\right).$$

Оттук и от (37) следва

$$Z_m=\frac{1}{\varphi(q)}M(\beta)+O\left(Ne^{-c\sqrt{\log N}}\right). \tag{38}$$

Заместваме последния израз за Z_m в (32) и вземаме предвид (17) и условието $q\le Q$. След като за пореден път предефинираме константата c, намираме

$$S\left(\frac{a}{q}+\beta\right)=\frac{1}{\varphi(q)}M(\beta)\sum_{\substack{m=0\\(m,q)=1}}^{q-1} e\left(\frac{am}{q}\right)+O\left(Ne^{-c\sqrt{\log N}}\right).$$

Остава да забележим, че сумата по m в горната формула е равна на сумата на Рамануджан $c_a(q)$, определена в Допълнението чрез формула (280). Тъй като от (27) ни е известно, че $(a,q)=1$, то като използваме Лема 45 виждаме, че в нашия случай е изпълнено $c_a(q)=\mu(q)$. С това доказателството на Лема 4 е завършено. □

Продължение на изледването на $R_1(n)$. Сега ще приложим формулата от Лема 4. От (29) веднага следва, че $|M(\beta)|\le N$ и поради това

$$S^2\left(\frac{a}{q}+\beta\right)=\frac{\mu^2(q)}{\varphi^2(q)}M^2(\beta)+O\left(N^2e^{-c\sqrt{\log N}}\right).$$

Като умножим двете страни на последното равенство с $e\left(-n(a/q+\beta)\right)$ и интегрираме по β получаваме, че за интеграла $H_{a,q}(n)$, определен чрез (26), е изпълнено

$$H_{a,q}(n)=\frac{\mu^2(q)}{\varphi^2(q)}e\left(-\frac{na}{q}\right)\int\limits_{-1/(q\tau)}^{1/(q\tau)}M^2(\beta)e(-n\beta)\,d\beta+O\left(\frac{N^2}{q\tau}e^{-c\sqrt{\log N}}\right). \tag{39}$$

Заместваме този израз в (25) и използваме определението на сумата на Рамануджан $c_n(q)$, дадено във формула (280), а също така очевидното равенство $c_{-n}(q)=c_n(q)$. Получаваме

$$R_1(n)=\sum_{q\le Q}\frac{\mu^2(q)}{\varphi^2(q)}\sum_{\substack{a=0\\(a,q)=1}}^{q-1}e\left(-\frac{na}{q}\right)\Gamma(n,q)+O\left(\Delta\right)$$

$$=\sum_{q\le Q}\frac{\mu^2(q)}{\varphi^2(q)}\,c_n(q)\,\Gamma(n,q)+O\left(\Delta\right), \tag{40}$$

където

$$\Gamma(n,q)=\int\limits_{-1/(q\tau)}^{1/(q\tau)}M^2(\beta)e(-n\beta)\,d\beta,\qquad\qquad \Delta=\sum_{q\le Q}\sum_{a=0}^{q-1}\frac{N^2}{q\tau}e^{-c\sqrt{\log N}}.$$

От (17) веднага следва

$$\Delta\ll\frac{QN^2}{\tau}e^{-c\sqrt{\log N}}\ll Ne^{-c\sqrt{\log N}}. \tag{41}$$

(Тук отново предефинирахме константата c.)

За да продължим по-нататък, ще използваме следната

Лема 5. *Нека $M\in\mathbb{Z}, H\in\mathbb{N}$, $\alpha\in\mathbb{R}$ и нека $||\alpha||$ е разстоянието от α до най-близкото цяло число. Тогава за сумата*

$$K(\alpha)=\sum_{k=M+1}^{M+H}e(\alpha k) \tag{42}$$

е в сила неравенството

$$|K(\alpha)| \le \min\left(H, \frac{1}{||\alpha||}\right). \tag{43}$$

Доказателство. От неравенството на триъгълника (Лема 29) и от Лема 27, свойство (3) веднага получаваме, че $|K(\alpha)| \le H$. Остава да докажем, че

$$|K(\alpha)| \le \frac{1}{||\alpha||} \qquad \text{при} \qquad \alpha \notin \mathbb{Z}.$$

От Лема 27 и от определението на $||\alpha||$ се вижда, че функциите $|K(\alpha)|$ и $||\alpha||^{-1}$ са четни, а също периодични с период 1. Следователно, достатъчно е да докажем, че

$$|K(\alpha)| \le \frac{1}{\alpha} \qquad \text{при} \qquad 0 < \alpha \le \frac{1}{2}. \tag{44}$$

Като се възползваме от определението на $e(\alpha)$, от Лема 27 и от формулата за сумата от членовете на геометрична прогресия, намираме

$$|K(\alpha)| = \left| e(\alpha(M+1)) \frac{1 - e(\alpha H)}{1 - e(\alpha)} \right| = \left| \frac{1 - e(\alpha H)}{1 - e(\alpha)} \right| \le \frac{2}{\left| e\left(-\frac{\alpha}{2}\right) - e\left(\frac{\alpha}{2}\right) \right|} = \frac{1}{\sin(\pi\alpha)}.$$

Остава да забележим, че функцията $\sin(\pi\alpha)$ е вдлъбната при $0 \le \alpha \le \frac{1}{2}$ откъдето $\sin(\pi\alpha) \ge 2\alpha$. Оттук (44) следва непосредствено, с което лемата е доказана. □

Да продължим с изучаването на $R_1(n)$. Вследствие на оценката от Лема 5, величината $|M(\beta)|$ е „малка“ ако β не е близко до цяло число. Оттук следва, че интегралът $\Gamma(n, q)$ е „близък“ до

$$\Gamma(n) = \int\limits_{-1/2}^{1/2} M^2(\beta) e(-n\beta)\, d\beta \tag{45}$$

По-точно, от Лема 5 следва, че $|M(\beta)| \le 1/|\beta|$ при $0 < |\beta| \le 1/2$ и тогава имаме

$$|\Gamma(n, q) - \Gamma(n)| \le \int\limits_{1/(q\tau) \le \beta \le 1/2} \left| M^2(\beta) \right| d\beta \le \int\limits_{1/(q\tau) \le \beta \le 1/2} \frac{d\beta}{\beta^2} \ll \int\limits_{1/(q\tau)}^{\infty} \frac{d\beta}{\beta^2} \ll q\tau. \tag{46}$$

Интегралът $\Gamma(n)$, дефиниран чрез (45), се изчислява лесно. Като използваме допускането $n \le N$, определението (29) и Лема 27, (свойства (4), (5)), намираме

$$\Gamma(n) = \int\limits_{-1/2}^{1/2} \sum_{m_1, m_2 \le N} e(\alpha m_1)\, e(\alpha m_2)\, e(-\alpha n)\, d\alpha$$

$$= \sum_{m_1, m_2 \le N} \int\limits_{-1/2}^{1/2} e(\alpha(m_1 + m_2 - n))\, d\alpha = \sum_{m_1 + m_2 = n} 1$$

$$= n - 1. \tag{47}$$

От (46) и (47) следва

$$\Gamma(n,q) = n + O(q\tau)$$

и като се възползваме от (40), (41), от очевидното неравенство $|c_n(q)| \leq \varphi(q)$ (виж формула (280)), намираме

$$R_1(n) = \sum_{q\leq Q} \frac{\mu^2(q)}{\varphi^2(q)} c_n(q)\left(n + O(q\tau)\right) + O\left(Ne^{-c\sqrt{\log n}}\right)$$

$$= n\mathfrak{S}(n;Q) + O\left(\tau \sum_{q\leq Q} \frac{q}{\varphi(q)}\right) + O\left(Ne^{-c\sqrt{\log n}}\right), \tag{48}$$

където при $X \geq 1$ сме определили

$$\mathfrak{S}(n;X) = \sum_{q\leq X} \lambda_n(q), \qquad \lambda_n(q) = \frac{\mu^2(q)}{\varphi^2(q)} c_n(q). \tag{49}$$

Като използваме (17) виждаме, че първият остатъчен член в (48) е

$$\ll \tau Q^2 \ll \frac{N}{(\log N)^{A_2-2A_1}}.$$

Лесно се вижда, че последният израз мажорира втория остатъчен член в (48). Тогава

$$R_1(n) = n\mathfrak{S}(n;Q) + O\left(\frac{N}{(\log N)^{A_2-2A_1}}\right). \tag{50}$$

Изследване на сумата $\mathfrak{S}(n;X)$. Ще докажем следната

Лема 6. *Функцията $\lambda_n(q)$ е мултипликативна по отношение на q. Редът*

$$\sum_{q=1}^{\infty} \lambda_n(q)$$

е абсолютно сходящ и при всяко $X \geq 2$ е изпълнено

$$\sum_{q>X} |\lambda_n(q)| \ll \frac{(\log N)(\log X)}{X}\,\tau(n), \tag{51}$$

където $\tau(n)$ е броя на положителните делители на n.

Доказателство. Мултипликативността на $\lambda_n(q)$ по отношение на q е очевидно следствие от Леми 39, 41 и 45.

За да докажем абсолютната сходимост на дадения ред и неравенството (51) ще оценим при $2 \leq X < Y$ сумата

$$F(X,Y) = \sum_{X<q\leq Y} |\lambda_n(q)| \tag{52}$$

и ще установим, че тя е произволно малка стига X да е достатъчно голямо — така ще можем да приложим необходимото и достатъчно условие на Коши за сходимост на безкраен ред.

От (49) и Леми 43, 45 следва, че

$$F(X,Y) \leq \sum_{X<q\leq Y} \frac{1}{\varphi(q)\,\varphi(\frac{q}{(q,n)})} \ll \sum_{X<q\leq Y} \frac{\log q}{q^2}\,(q,n).$$

Разделяме последната сума на части съобразно стойността на най-големия общ делител (q,n) и получаваме

$$F(X,Y) \ll \sum_{d|n} d \sum_{\substack{X<q\leq Y \\ q\equiv 0 \pmod d}} \frac{\log q}{q^2} \ll \sum_{d|n} d \sum_{X/d<m\leq Y/d} \frac{\log(md)}{m^2d^2}.$$

Като използваме очевидното неравенство $\log(md) \ll \log(2m)\log(2d)$ и условието $n \leq N$, намираме

$$F(X,Y) \ll \sum_{d|n} \frac{\log(2d)}{d} \sum_{X/d<m\leq Y/d} \frac{\log(2m)}{m^2} \ll (\log N) \sum_{d|n} \frac{1}{d} \sum_{X/d<m} \frac{\log(2m)}{m^2}. \qquad (53)$$

(Да отбележим, че редът $\sum_{m=1}^{\infty} \frac{\log(2m)}{m^2}$ е сходящ.)

Лесно се доказва, че

$$\sum_{m>Z} \frac{\log(2m)}{m^2} \ll \frac{\log(2Z)}{Z} \qquad \text{при} \qquad Z \geq 1. \qquad (54)$$

Наистина, при $1 \leq Z \leq 2$ оценката (54) е очевидна, а при $Z > 2$ имаме

$$\sum_{m>Z} \frac{\log(2m)}{m^2} \ll \frac{\log Z}{Z} + \int_Z^{\infty} \frac{\log(2x)}{x^2}\,dx \ll \frac{\log Z}{Z} + \int_Z^{Z^2} \frac{\log(2x)}{x^2}\,dx + \int_{Z^2}^{\infty} \frac{\log(2x)}{x^2}\,dx$$

$$\ll \frac{\log Z}{Z} + (\log Z)\int_Z^{\infty} \frac{dx}{x^2} + \int_{Z^2} \frac{dx}{x^{3/2}} \ll \frac{\log Z}{Z}.$$

Да се върнем към израза в дясната част на (53). Разделяме сумата по d на две части, съответно по $d > X$ и $d \le X$. Като използваме (54), получаваме

$$F(X,Y) \ll (\log N) \left(\sum_{\substack{d|n \\ d>X}} \frac{1}{d} + \sum_{\substack{d|n \\ d\le X}} \frac{1}{d} \, \frac{\log(2X/d)}{X/d} \right)$$

$$\ll (\log N) \left(\frac{1}{X} \sum_{\substack{d|n \\ d>X}} 1 + \frac{\log X}{X} \sum_{\substack{d|n \\ d\le X}} 1 \right)$$

$$\ll \frac{(\log N)(\log X)}{X} \, \tau(n). \tag{55}$$

Последният израз не зависи от Y и клони към 0 при $X \to \infty$. Следователно редът $\sum_{q=1}^{\infty} \lambda_n(q)$ е абсолютно сходящ. Използваме (52) и (55) и, като извършим граничен преход $Y \to \infty$, получаваме (51). Лемата е доказана. $\square$

Като приложим Лема 6, тъждеството на Ойлер (Лема 35) и вземем предвид определенията (6) и (49), съответно на $\mathfrak{S}(n)$ и $\lambda_n(q)$, и свойствата на функциите на Мьобиус, Ойлер и Рамануджан, получаваме

$$\sum_{q=1}^{\infty} \lambda_n(q) = \prod_p \big(1 + \lambda_n(p) + \lambda_n(p^2) + \dots\big)$$

$$= \prod_p (1 + \lambda_n(p))$$

$$= \prod_{p\nmid n} (1 + \lambda_n(p)) \prod_{p|n} (1 + \lambda_n(p))$$

$$= \prod_{p\nmid n} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{p|n} \left(1 + \frac{1}{p-1}\right)$$

$$= \mathfrak{S}(n). \tag{56}$$

От (17), (49), (56) и Лема 6 следва

$$\mathfrak{S}(n;Q) = \mathfrak{S}(n) + O\left(\frac{\tau(n)}{(\log N)^{A_1-2}}\right). \tag{57}$$

Оценка за $\mathcal{E}_1$. Като заместим израза от дясната част на (57) в (50), намираме

$$R_1(n) = n\mathfrak{S}(n) + O\left(\frac{N\,\tau(n)}{(\log N)^{A_1-2}}\right) + O\left(\frac{N}{(\log N)^{A_2-2A_1}}\right).$$

От (24) и от последната формула следва

$$\mathcal{E}_1 \ll \sum_{n\le N}\left(\frac{N^2\,\tau^2(n)}{(\log N)^{2A_1-4}} + \frac{N^2}{(\log N)^{2A_2-4A_1}}\right)$$

$$\ll \frac{N^2}{(\log N)^{2A_1-4}}\sum_{n\le N}\tau^2(n) + \frac{N^3}{(\log N)^{2A_2-4A_1}}.$$

Остава да приложим Лема 38 и получаваме

$$\mathcal{E}_1 \ll \frac{N^3}{(\log N)^{2A_1-7}} + \frac{N^3}{(\log N)^{2A_2-4A_1}}. \tag{58}$$

2.2.3 Оценяване на $\mathcal{E}_2$.

Начало. От (22), (24) и от неравенството на Бесел (Лема 33), приложено към функцията

$$f(\alpha) = \begin{cases} S^2(\alpha) & \text{при} \quad \alpha\in\mathfrak{m}, \\ 0 & \text{при} \quad \alpha\in\mathfrak{M} \end{cases}$$

следва, че

$$\mathcal{E}_2 = \sum_{n\le N}\left|\int\limits_{\mathfrak{m}} S^2(\alpha)\,e(-\alpha n)\,d\alpha\right|^2 \le \int\limits_{\mathfrak{m}} |S(\alpha)|^4\,d\alpha \le \left(\sup_{\alpha\in\mathfrak{m}}|S(\alpha)|\right)^2\int\limits_{\mathfrak{m}}|S(\alpha)|^2\,d\alpha. \tag{59}$$

По-нататък от (20) следва, че $\mathfrak{m}\subset\left[-\frac{1}{\tau}, 1-\frac{1}{\tau}\right]$. Тогава

$$\int\limits_{\mathfrak{m}}|S(\alpha)|^2\,d\alpha \le \int\limits_{-1/\tau}^{1-1/\tau}|S(\alpha)|^2\,d\alpha = \int\limits_0^1|S(\alpha)|^2\,d\alpha. \tag{60}$$

Тук използвахме, че подинтегралната функция е периодична с период 1. Като вземем предвид (15), свойства (4) и (5) от Лема 27 и теоремата на Чебишев (Лема 52), намираме

$$\int_0^1 |S(\alpha)|^2 \, d\alpha = \int_0^1 \sum_{p_1, p_2 \le N} (\log p_1)(\log p_2)\, e(\alpha(p_1 - p_2))\, d\alpha$$

$$= \sum_{p_1, p_2 \le N} (\log p_1)(\log p_2) \int_0^1 e(\alpha(p_1 - p_2))\, d\alpha$$

$$= \sum_{\substack{p_1, p_2 \le N \\ p_1 - p_2 = 0}} (\log p_1)(\log p_2) = \sum_{p \le N} (\log p)^2 \ll \pi(N)\, (\log N)^2$$

$$\ll N \, \log N. \tag{61}$$

От (59), (60) и (61) следва

$$\mathcal{E}_2 \ll \left(\sup_{\alpha \in \mathfrak{m}} |S(\alpha)| \right)^2 N\, (\log N). \tag{62}$$

И така, остава да се оцени $S(\alpha)$ равномерно по $\alpha \in \mathfrak{m}$. Това ще извършим в следващите параграфи.

Методът на Виноградов. Нека имаме сума по прости числа

$$\sum_{p \le x} f(p),$$

където f е дадена функция. (В приложенията тя обикновено е „осцилираща“.) Виноградов е показал, че всяка такава сума може да се представи като линейна комбинация на няколко суми от два типа.

Сумите от първи тип са двойни суми от вида

$$\sum_{\substack{dl \le x \\ d \le u}} \gamma_d \, f(dl).$$

Тук параметърът u нараства заедно с x, но доста по-бавно от x, а числата γ_d са „малки“. Тъй като няма коефициенти, зависещи от l, то тези суми се оценяват добре, ако се използва осцилацията на f.

Сумите от втори тип са двойни суми от вида

$$\sum_{\substack{dl \le x \\ d > u \\ l > u}} \gamma_d \, \delta_l \, f(dl).$$

Тук коефициентите γ_d, δ_l са „малки“, но това не ни дава възможност да използваме директно осцилационното свойство на f. Това обаче може да се извърши по друг начин. За да илюстрираме метода нека разгледаме по-простата сума от втори тип

$$\mathcal{H} = \sum_{\substack{D<d\le 2D \\ L<l\le 2L}} \gamma_d \, \delta_l \, f(dl),$$

където $DL \le x, D \ge u, L \ge u$ и нека считаме, че $|\gamma_d| \le 1, |\delta_l| \le 1$. Като използваме неравенството на триъгълника (Лема 29) получаваме

$$|\mathcal{H}| \le \sum_{D<d\le 2D} \left| \sum_{L<l\le 2L} \delta_l \, f(dl) \right| .$$

По този начин се освободихме от изразите γ_d. Сега прилагаме неравенството на Коши (Лема 30) и използваме, че при $z \in \mathbb{C}$ е изпълнено $|z|^2 = z\overline{z}$, където $\overline{z}$ е комплексното спрегнато на z. След това сменяме реда на сумиране и получаваме

$$\begin{aligned} |\mathcal{H}|^2 &\le D \sum_{D<d\le 2D} \left| \sum_{L<l\le 2L} \delta_l \, f(dl) \right|^2 \\ &= \sum_{D<d\le 2D} \; \sum_{L<l_1\le 2L} \delta_{l_1} \, f(dl) \sum_{L<l_2\le 2L} \overline{\delta_{l_2}} \, \overline{f(dl)} \\ &= \sum_{L<l_1\le 2L} \; \sum_{L<l_2\le 2L} \delta_{l_1} \, \overline{\delta_{l_2}} \sum_{D<d\le 2D} f(dl) \, \overline{f(dl)}. \end{aligned}$$

Оттук следва

$$|\mathcal{H}|^2 \le \sum_{L<l_1\le 2L} \; \sum_{L<l_2\le 2L} \left| \sum_{D<d\le 2D} f(dl) \, \overline{f(dl)} \right| .$$

По този начин се освободихме и от δ_l. Сега, ако използваме умело осцилационните свойства на f, ще получим нетривиална оценка за $\mathcal{H}$.

Тъждество на Вон. Следващата лема, известна като *тъждество на Вон*, ни дава представяне на дадена сума по прости числа чрез линейна комбинация на две суми от първи тип и една сума от втори тип. Ще отбележим, че оригиналният метод на Виноградов е значително по-сложен.

Лема 7. *Нека $x, u \in \mathbb{R}$, $1 < u < x$, нека $f(n)$ е произволна функция, дефинирана за $n \in \mathbb{N}, n \le x$ и нека $\Lambda(n)$, $\mu(n)$, $\tau(n)$ са съответно функцията на Манголд, функцията на Мьобиус и броя на положителните делители на n. В сила е тъждеството*

$$\sum_{u<n\le x} \Lambda(n) f(n) = W_1 - W_2 - W_3, \tag{63}$$

където

$$W_1 = \sum_{d \le u} \mu(d) \sum_{l \le \frac{x}{d}} (\log l) \, f(dl), \tag{64}$$

$$W_2 = \sum_{d \le u^2} c(d) \sum_{l \le \frac{x}{d}} f(dl), \tag{65}$$

$$W_3 = \sum_{u < d \le \frac{x}{u}} \sum_{u < l \le \frac{x}{d}} a(d) \, \Lambda(l) \, f(dl), \tag{66}$$

и където

$$a(d) = \sum_{\substack{k | d \\ k \le u}} \mu(k), \qquad c(d) = \sum_{\substack{kh = d \\ k \le u \\ h \le u}} \mu(k) \, \Lambda(h). \tag{67}$$

Освен това, изпълнени са неравенствата

$$|a(d)| \le \tau(d), \qquad |c(d)| \le \log d. \tag{68}$$

Доказателство. При $u < n$ използваме Лема 44 и записваме $\Lambda(n)$ във вида

$$\Lambda(n) = \sum_{d | n} \mu(d) \log \frac{n}{d} = \sum_{dl = n} \mu(d) \log l = I(n) + I'(n), \tag{69}$$

където

$$I(n) = \sum_{\substack{dl = n \\ d \le u}} \mu(d) \log l, \qquad I'(n) = \sum_{\substack{dl = n \\ d > u}} \mu(d) \log l. \tag{70}$$

Да разгледаме $I'(n)$. Като използваме отново Лема 44 записваме

$$I'(n) = \sum_{\substack{dl = n \\ d > u}} \mu(d) \sum_{k | l} \Lambda(k) = \sum_{\substack{dl = n \\ d > u}} \mu(d) \sum_{kr = l} \Lambda(k) = \sum_{\substack{dkr = n \\ d > u}} \mu(d) \Lambda(k).$$

Разделяме последната сума на две части съобразно големината на k. Получаваме

$$I'(n) = I''(n) + I^*(n), \tag{71}$$

където

$$I''(n) = \sum_{\substack{dkr = n \\ d > u \\ k \le u}} \mu(d) \Lambda(k), \qquad I^*(n) = \sum_{\substack{dkr = n \\ d > u \\ k > u}} \mu(d) \Lambda(k). \tag{72}$$

Да разгледаме $I''(n)$. Имаме

$$I''(n) = I'''(n) - J(n), \tag{73}$$

където

$$I'''(n) = \sum_{\substack{dkr=n \\ k\le u}} \mu(d)\Lambda(k), \qquad J(n) = \sum_{\substack{dkr=n \\ d\le u \\ k\le u}} \mu(d)\Lambda(k). \tag{74}$$

Но

$$I'''(n) = \sum_{\substack{sk=n \\ k\le u}} \Lambda(k) \sum_{dr=s} \mu(d) = 0, \tag{75}$$

тъй като вътрешната сума в горния израз е равна на $\sum_{d|s}\mu(d) = 0$ (използвахме Лема 40). По-нататък, очевидно можем да запишем сумата $J(n)$ като

$$J(n) = \sum_{\substack{mr=n \\ m\le u^2}} \left(\sum_{\substack{dk=m \\ d\le u \\ k\le u}} \mu(d)\Lambda(k) \right) = \sum_{\substack{mr=n \\ m\le u^2}} c(m), \qquad c(m) = \sum_{\substack{dk=m \\ d\le u \\ k\le u}} \mu(d)\Lambda(k). \tag{76}$$

Сега да разгледаме $I^*(n)$, определено чрез (72). Записваме го във вида

$$I^*(n) = \sum_{\substack{tk=n \\ t>u \\ k>u}} \left(\sum_{\substack{dr=t \\ d>u}} \mu(d) \right) \Lambda(k) = \sum_{\substack{tk=n \\ t>u \\ k>u}} \left(\sum_{dr=t} \mu(d) - \sum_{\substack{dr=t \\ d\le u}} \mu(d) \right) \Lambda(k) = -K(n), \tag{77}$$

където

$$K(n) = \sum_{\substack{tk=n \\ t>u \\ k>u}} \left(\sum_{\substack{dr=t \\ d\le u}} \mu(d) \right) \Lambda(k) = \sum_{\substack{tk=n \\ t>u \\ k>u}} a(t)\,\Lambda(k), \qquad a(t) = \sum_{\substack{dr=t \\ d\le u}} \mu(d). \tag{78}$$

Като използваме (69), (71), (73), (75) и (77), записваме

$$\Lambda(n) = I(n) - J(n) - K(n) \qquad \text{при} \qquad u < n, \tag{79}$$

където събираемите в дясната част на последното равенство се определят чрез (70), (76) и (78). След като сменим, за удобство, сумационните променливи, можем да запишем

$$I(n) = \sum_{\substack{dl=n \\ d\le u}} \mu(d)\log l, \qquad J(n) = \sum_{\substack{dl=n \\ d\le u^2}} c(d), \qquad K(n) = \sum_{\substack{dl=n \\ d>u \\ l>u}} a(d)\,\Lambda(l), \tag{80}$$

където $a(d)$, $c(d)$ се задават чрез (67). Да отбележим, че величините в дясната част на (79) имат смисъл и при $n \le u$, като в този случай от Лема 40 и Лема 44 непосредствено следва, че $I(n) = J(n) = \Lambda(n)$, $K(n) = 0$. Или намираме

$$0 = I(n) - J(n) - K(n) \qquad \text{при} \qquad n \le u. \tag{81}$$

Умножаваме двете страни на (79) и (81) с $f(n)$ и сумираме по n. Като използваме (80), получаваме

$$\sum_{u<n\leq x} \Lambda(n)f(n) = W_1' - W_2' - W_3',$$

като

$$W_1' = \sum_{n\leq x} I(n)f(n) = \sum_{\substack{dl\leq x\\ d\leq u}} \mu(d)\,(\log l)\,f(dl) = W_1,$$

$$W_2' = \sum_{n\leq x} J(n)f(n) = \sum_{\substack{dl\leq x\\ d\leq u^2}} c(d)\,f(dl) = W_2,$$

$$W_3' = \sum_{n\leq x} K(n)f(n) = \sum_{\substack{dl\leq x\\ d>u\\ l>u}} a(d)\,\Lambda(l)\,f(dl) = W_3.$$

С това равенството (63) е доказано.

Остава да проверим (68). От Лема 44 следва

$$|c(d)| \leq \sum_{kh=d} \Lambda(h) = \sum_{h|d} \Lambda(h) = \log d$$

и очевидно

$$|a(d)| \leq \sum_{k|d} 1 = \tau(d).$$

С това лемата е доказана. □

Една елементарна лема.

Лема 8. *Нека* $X, Y \in \mathbb{R}, X \geq 1, Y \geq 1; \alpha \in \mathbb{R}, a \in \mathbb{Z}, q \in \mathbb{N}$ *и нека*

$$\left|\alpha - \frac{a}{q}\right| \leq \frac{1}{q^2}, \qquad (a,q) = 1. \tag{82}$$

Разглеждаме сумата

$$U = \sum_{n\leq X} \min\left(\frac{XY}{n}, \frac{1}{||\alpha n||}\right), \tag{83}$$

където $||x||$ *е разстоянието от* x *до най-близкото цяло число. Тогава за сумата* U *е изпълнено неравенството*

$$U \leq 100\, XY \left(\frac{1}{q} + \frac{1}{Y} + \frac{q}{XY}\right) \log(3qX). \tag{84}$$

Доказателство. Първо да отбележим, че от известната оценка

$$\sum_{n\leq x}\frac{1}{n}\leq 1+\log x \qquad \text{при} \qquad x\geq 1 \tag{85}$$

следват неравенствата

$$U\leq\sum_{n\leq X}\frac{XY}{n}\leq XY(1+\log X)\leq XY\log(3X).$$

Ако $q\leq 100$, то от последното неравенство следва (84). Оттук нататък ще предполагаме, че $q>100$.

Нека разгледаме сумата

$$V_0=\sum_{n\leq\frac{q}{2}}\min\left(\frac{XY}{n},\frac{1}{||\alpha n||}\right). \tag{86}$$

От (82) следва, че α може да се запише във вида

$$\alpha=\frac{a}{q}+\frac{\theta}{q^2}, \qquad |\theta|\leq 1. \tag{87}$$

Да отбележим, че функцията $||x||$ е периодична с период 1 и са изпълнени условията

$$||x+y||\leq||x||+||y|| \qquad \text{и} \qquad ||x||=|x| \quad \text{при} \quad |x|\leq\frac{1}{2}. \tag{88}$$

Тъй като $(a,q)=1$, то при $1\leq n\leq\frac{q}{2}$ имаме $q\nmid an$, следователно $||\frac{an}{q}||\geq\frac{1}{q}$. Тогава, като вземем предвид (87), (88) и условието $n\leq q/2$, получаваме

$$||\alpha n||=\left|\left|\frac{an}{q}+\frac{\theta n}{q^2}\right|\right|\geq\left|\left|\frac{an}{q}\right|\right|-\left|\left|\frac{\theta n}{q^2}\right|\right|\geq\left|\left|\frac{an}{q}\right|\right|-\frac{|\theta n|}{q^2}\geq\left|\left|\frac{an}{q}\right|\right|-\frac{1}{2q}\geq\frac{1}{2}\left|\left|\frac{an}{q}\right|\right|. \tag{89}$$

От горното неравенство и от (85), (86), (88) и (89) следва

$$\begin{aligned}V_0&\leq\sum_{n\leq\frac{q}{2}}\frac{1}{||\alpha n||}\leq 2\sum_{n\leq\frac{q}{2}}\left|\left|\frac{an}{q}\right|\right|^{-1}=2\sum_{\substack{-\frac{q}{2}<l\leq\frac{q}{2}\\ l\neq 0}}\ \sum_{\substack{n\leq\frac{q}{2}\\ an\equiv l \pmod q}}\left|\left|\frac{an}{q}\right|\right|^{-1}\\&=2\sum_{\substack{-\frac{q}{2}<l\leq\frac{q}{2}\\ l\neq 0}}\left|\frac{l}{q}\right|^{-1}\sum_{\substack{n\leq\frac{q}{2}\\ an\equiv l \pmod q}}1\ \leq\ 4q\sum_{1\leq l\leq\frac{q}{2}}\frac{1}{l}\\&\leq 4q\log(3q).\end{aligned} \tag{90}$$

Ако $X\leq\frac{q}{2}$, то очевидно $U\leq V_0$ и от (90) следва неравенството (84).

Сега да разгледаме случая $X > \frac{q}{2}$. Тогава имаме

$$U \leq V_0 + \sum_{s=0}^{k} W_s, \tag{91}$$

където

$$W_s = \sum_{\left(s+\frac{1}{2}\right)q < n \leq \left(s+\frac{3}{2}\right)q} \min\left(\frac{XY}{n}, \frac{1}{||\alpha n||}\right), \tag{92}$$

а k се определя от условията

$$\left(k+\frac{1}{2}\right)q \leq X < \left(k+\frac{3}{2}\right)q.$$

Ясно е, че

$$k = \left[\frac{X}{q} - \frac{1}{2}\right] \leq \frac{X}{q}. \tag{93}$$

Записваме W_s във вида

$$W_s = \sum_{-\frac{q}{2} < l \leq \frac{q}{2}} \min\left(\frac{XY}{(s+1)q+l}, \frac{1}{||\alpha((s+1)q+l)||}\right).$$

От (87) следва

$$\alpha((s+1)q+l) = \left(\frac{a}{q} + \frac{\theta}{q^2}\right)((s+1)q+l)$$

$$= a(s+1) + \frac{al}{q} + \frac{\theta(s+1)}{q} + \frac{\theta l}{q^2}$$

$$= a(s+1) + \frac{al + [\theta(s+1)]}{q} + \frac{\lambda(l)}{q}, \tag{94}$$

където

$$\lambda(l) = \lambda_{q,s,\theta}(l) = \{\theta(s+1)\} + \frac{\theta l}{q}.$$

Като използваме (87) и условието $-\frac{q}{2} < l \leq \frac{q}{2}$ виждаме, че

$$|\lambda(l)| < 2.$$

Тогава от (88) и (94) получаваме

$$||\alpha((s+1)q+l)|| = \left|\left|\frac{al + [\theta(s+1)]}{q} + \frac{\lambda(l)}{q}\right|\right|$$

$$\geq \left|\left|\frac{al + [\theta(s+1)]}{q}\right|\right| - \left|\frac{\lambda(l)}{q}\right|$$

$$\geq \left|\left|\frac{al + [\theta(s+1)]}{q}\right|\right| - \frac{2}{q}. \tag{95}$$

Разделяме W_s на две части

$$W_s = W_s' + W_s'', \tag{96}$$

където в W_s' са събираемите, за които

$$al + [\theta(s+1)] \equiv 0, \pm 1, \pm 2 \pmod q,$$

а W_s'' съдържа останалите събираеми.

Сумата W_s' съдържа не повече от 5 члена и всеки от тях не надхвърля $\frac{XY}{(s+1)q - q/2}$. Тогава

$$W_s' \leq \frac{5XY}{(s+\frac{1}{2})q}. \tag{97}$$

Сега да разгледаме W_s''. Стойностите, които сумационната променлива l на тази сума пробягва, са такива, че

$$al + [\theta(s+1)] \equiv m \pmod q,$$

където $3 \leq |m| \leq \frac{q}{2}$. Тогава, за всяко такова l изразът в последния ред на (95) е положителен. Следователно

$$W_2'' \leq \sum_{3 \leq |m| \leq \frac{q}{2}} \sum_{\substack{-\frac{q}{2} < l \leq \frac{q}{2} \\ al + [\theta(s+1)] \equiv m \pmod q}} \frac{1}{\left|\left|\frac{al+[\theta(s+1)]}{q}\right|\right| - \frac{2}{q}}$$

$$\leq \sum_{3 \leq |m| \leq \frac{q}{2}} \frac{1}{\frac{|m|}{q} - \frac{2}{q}}$$

$$\leq 2q \sum_{3 \leq m \leq \frac{q}{2}} \frac{1}{m-2}.$$

От горното неравенство и от (85) получаваме

$$W_2'' \leq 2q \log(3q). \tag{98}$$

От (96), (97), (98) следва

$$W_s \leq \frac{5XY}{q\left(s+\frac{1}{2}\right)} + 2q\log(3q)$$

и тогава, като вземем предвид (85) и (93), намираме

$$\sum_{s=0}^{k} W_s \leq \frac{5XY}{q} \sum_{s=0}^{k} \frac{1}{s+\frac{1}{2}} + 2(k+1)q\log(3q)$$

$$\leq \frac{5XY}{q}(3 + \log k) + 2\left(\frac{X}{q} + 1\right) q \log(3q)$$

$$\leq 50\left(\frac{XY}{q} + X + q\right)\log(3qX). \tag{99}$$

Неравенството (84) е следствие на (90), (91) и (99). Лемата е доказана. □

Оценяване на $S(\alpha)$. Ще докажем следната основна

Лема 9. *Нека $\alpha \in \mathbb{R}$, $a \in \mathbb{Z}$, $q \in \mathbb{N}$, като*

$$\left|\alpha - \frac{a}{q}\right| \le \frac{1}{q^2}, \qquad (a,q) = 1, \qquad q \le N. \tag{100}$$

Тогава за сумата

$$S(\alpha) = \sum_{p \le N} (\log p)\, e(\alpha p)$$

е изпълнено

$$|S(\alpha)| \ll \left(N q^{-\frac{1}{2}} + N^{\frac{4}{5}} + N^{\frac{1}{2}} q^{\frac{1}{2}} \right) (\log N)^4. \tag{101}$$

Доказателство. Разглеждаме сумата

$$S^*(\alpha) = \sum_{n \le N} \Lambda(n)\, e(\alpha n).$$

Като използваме определението на функцията на Манголд получаваме

$$S^*(\alpha) = \sum_{p^l \le N} (\log p)\, e\left(\alpha p^l\right) = S(\alpha) + \Delta',$$

където

$$\Delta' = \sum_{\substack{p^l \le N \\ l \ge 2}} (\log p)\, e\left(\alpha p^l\right).$$

В сумата, определяща Δ', сумационната променлива l пробягва най много $O(\log N)$ стойности и най-голямото събираемо (отговарящо на $l = 2$) има порядък $O(\sqrt{N})$. Следователно $\Delta' = O\left(\sqrt{N} \log N\right)$, откъдето следва

$$S(\alpha) = S^*(\alpha) + O\left(\sqrt{N} \log N\right). \tag{102}$$

За да оценим $S^*(\alpha)$ въвеждаме параметър u, който ще изберем по-късно. Засега считаме само, че u удовлетворява условието

$$1 < u < \sqrt{N}. \tag{103}$$

Като се възползваме от тъждеството на Вон (Лема 7), получаваме

$$S^*(\alpha) = W_1 - W_2 - W_3 + O(u), \tag{104}$$

където

$$W_1 = \sum_{d \le u} \mu(d) \sum_{l \le \frac{N}{d}} (\log l)\, e(\alpha d l), \tag{105}$$

$$W_2 = \sum_{d \le u^2} c(d) \sum_{l \le \frac{N}{d}} e(\alpha d l), \tag{106}$$

$$W_3 = \sum_{u < d \le \frac{N}{u}} \sum_{u < l \le \frac{N}{d}} a(d)\, \Lambda(l)\, e(\alpha d l), \tag{107}$$

и където $a(d)$, $c(d)$ са реални числа, удовлетворяващи съответно условията

$$|a(d)| \le \tau(d), \qquad |c(d)| \le \log d. \tag{108}$$

Да оценим първо W_2. (Както отбелязахме преди, това е сума от първи тип.) От (106), (108) и Лема 5 следва

$$|W_2| \ll (\log N) \sum_{d \le u^2} \left| \sum_{l \le \frac{N}{d}} e(\alpha d l) \right| \ll (\log N) \sum_{d \le u^2} \min\left(\frac{N}{d}, \frac{1}{||\alpha d||} \right).$$

Прилагаме Лема 8 за параметрите $X = u^2$, $Y = N u^{-2}$ и получаваме

$$|W_2| \ll N \left(\frac{1}{q} + \frac{u^2}{N} + \frac{q}{N} \right) (\log N)^2. \tag{109}$$

Сега да разгледаме W_1. Тази величина не е сума от първи тип поради наличието на израза $(\log l)$, но лесно се свежда до такава с помощта на преобразованието на Абел (Лема 31). Преобразуваме вътрешната сума в (105) по формулата от Лема 31 след което прилагаме Лема 5. Получаваме

$$\left| \sum_{l \le \frac{N}{d}} (\log l)\, e(\alpha d l) \right| = \left| - \int_1^{N/d} \sum_{l \le t} e(\alpha d l)\ (\log t)'\, dt + \sum_{l \le \frac{N}{d}} e(\alpha d l)\ \log(N/d) \right|$$

$$\le \int_1^{N/d} \left| \sum_{l \le t} e(\alpha d l) \right| \ \frac{dt}{t} + \left| \sum_{l \le \frac{N}{d}} e(\alpha d l) \right| \log N$$

$$\le \min\left(\frac{N}{d}, \frac{1}{||\alpha d||} \right) \ \left(\int_1^{N/d} \frac{dt}{t} + \log N \right)$$

$$\ll \min\left(\frac{N}{d}, \frac{1}{||\alpha d||} \right) \ \log N.$$

Оттук, от (105) и от Лема 8 следва

$$|W_1| \ll (\log N) \sum_{d \le u} \min\left(\frac{N}{d}, \frac{1}{||\alpha d||}\right) \ll N\left(\frac{1}{q} + \frac{u}{N} + \frac{q}{N}\right)(\log N)^2. \tag{110}$$

Остава да оценим сумата от втори тип W_3, определена чрез (107). Първо разделяме интервала, който пробягва d, на части с помощта на точките $2^i u$, $i = 0, 1, 2, \ldots$. Получават се $O(\log N)$ подинтервала, като всеки от тях е от вида $(D, D_1]$, където

$$u \le D < D_1 \le \frac{N}{u}, \qquad D_1 \le 2D. \tag{111}$$

Следователно W_3 се разбива на $O(\log N)$ подсуми от вида

$$W^* = W^*(D, D_1) = \sum_{D < d \le D_1} \sum_{u < l \le \frac{N}{d}} a(d)\, \Lambda(l)\, e(\alpha d l),$$

където D и D_1 удовлетворяват (111). За да оценим W^* използваме (108) и прилагаме неравенството на триъгълника (Лема 29). Получаваме

$$|W^*| \le \sum_{D < d \le D_1} \tau(d) \left| \sum_{u < l \le \frac{N}{d}} \Lambda(l)\, e(\alpha d l) \right|.$$

Сега прилагаме неравенството на Коши (Лема 30), след което се възползваме от Лема 38 и условията (111). Намираме

$$|W^*|^2 \le \left(\sum_{D < d \le D_1} \tau^2(d) \right) \left(\sum_{D < d \le D_1} \left| \sum_{u < l \le \frac{N}{d}} \Lambda(l)\, e(\alpha d l) \right|^2 \right)$$

$$\ll (\log N)^3\, D \sum_{D < d \le D_1} \left| \sum_{u < l \le \frac{N}{d}} \Lambda(l)\, e(\alpha d l) \right|^2.$$

Към сумата по l в горния израз прилагаме тъждеството $|z|^2 = z\overline{z}$, където $\overline{z}$ е комплексното спрегнато на z, след което сменяме реда на сумиране. Получаваме

$$|W^*|^2 \ll (\log N)^3\, D \sum_{D < d \le D_1} \sum_{u < l_1 \le \frac{N}{d}} \sum_{u < l_2 \le \frac{N}{d}} \Lambda(l_1)\, \Lambda(l_2)\, e(\alpha d l_1)\, e(-\alpha d l_2)$$

$$= (\log N)^3\, D \sum_{u < l_1 \le \frac{N}{D}} \sum_{u < l_2 \le \frac{N}{D}} \Lambda(l_1)\, \Lambda(l_2) \sum_{D < d \le D_{l_1, l_2}} e(\alpha d (l_1 - l_2)),$$

където

$$D_{l_1, l_2} = \min(D_1, N/l_1, N/l_2) \le 2D. \tag{112}$$

Оттук следва

$$|W^*|^2 \ll (\log N)^5 \, D \, \Sigma, \tag{113}$$

където

$$\Sigma = \sum_{u \le l_1, l_2 \le \frac{N}{D}} \left| \sum_{D < d \le D_{l_1, l_2}} e(\alpha d(l_1 - l_2)) \right|. \tag{114}$$

Представяме тази сума във вида

$$\Sigma = \Sigma_1 + \Sigma_2, \tag{115}$$

където Σ_1 съдържа събираемите, за които $l_1 = l_2$, а Σ_2 събираемите, за които $l_1 \neq l_2$. Като оценим тривиално сумата по d, получаваме

$$\Sigma_1 \ll D \sum_{u < l \le \frac{N}{D}} 1 \ll N. \tag{116}$$

Да разгледаме Σ_2. Разделяме тази сума на части съобразно стойността на $l_1 - l_2$ и прилагаме Лема 5 и (112). Получаваме

$$\Sigma_2 = \sum_{1 \le |h| \le \frac{N}{D}} \sum_{\substack{u \le l_1, l_2 \le \frac{N}{D} \\ l_1 - l_2 = h}} \left| \sum_{D < d \le D_{l_1, l_2}} e(\alpha d(l_1 - l_2)) \right|$$

$$\ll \sum_{1 \le |h| \le \frac{N}{D}} \sum_{\substack{u \le l_1, l_2 \le \frac{N}{D} \\ l_1 - l_2 = h}} \min\left(D, \frac{1}{||\alpha h||}\right)$$

$$= \sum_{1 \le |h| \le \frac{N}{D}} \min\left(D, \frac{1}{||\alpha h||}\right) \sum_{\substack{u \le l_1, l_2 \le \frac{N}{D} \\ l_1 - l_2 = h}} 1$$

$$\ll \frac{N}{D} \sum_{1 \le h \le \frac{N}{D}} \min\left(D, \frac{1}{||\alpha h||}\right).$$

При $1 \le h \le \frac{N}{D}$ имаме $D \le \frac{N}{h}$. Тогава от горната формула и от Лема 8 получаваме

$$\Sigma_2 \ll \frac{N}{D} \sum_{1 \le h \le \frac{N}{D}} \min\left(\frac{N}{h}, \frac{1}{||\alpha(l_1 - l_2)||}\right) \ll \frac{N^2}{D}\left(\frac{1}{q} + \frac{1}{D} + \frac{q}{N}\right) \log N. \tag{117}$$

От (113), (115), (116) и (117) следва

$$|W^*|^2 \ll \left(DN + \frac{N^2}{q} + \frac{N^2}{D} + Nq\right) (\log N)^6.$$

Като вземем предвид долната и горната граници за D от (111), намираме

$$|W^*|^2 \ll \left(\frac{N^2}{u} + \frac{N^2}{q} + Nq\right)(\log N)^6,$$

откъдето

$$|W^*| \ll \left(\frac{N}{u^{1/2}} + \frac{N}{q^{1/2}} + N^{1/2}q^{1/2}\right)(\log N)^3.$$

Да си припомним, че сумата W_3 се състои от $O(\log N)$ суми от вида W^*. Тогава

$$|W_3| \ll \left(\frac{N}{u^{1/2}} + \frac{N}{q^{1/2}} + N^{1/2}q^{1/2}\right)(\log N)^4. \tag{118}$$

От (100), (102), (104), (109), (110) and (118) следва

$$|S(\alpha)| \ll \left(\frac{N}{u^{1/2}} + \frac{N}{q^{1/2}} + N^{1/2}q^{1/2} + u^2\right)(\log N)^4. \tag{119}$$

Избираме параметъра u така, че порядъкът на израза в дясната страна на горното неравенство да е минимален. Това се случва, ако $Nu^{-1/2} = u^2$, т.е. когато $u = N^{2/5}$. (При този избор на u условието (103) е изпълнено.) Тогава, като заместим $u = N^{2/5}$ в (119) получаваме (101), с което лемата е доказана. □

Оценка за $\mathcal{E}_2$. Вече сме в състояние да оценим $\sup_{\alpha\in\mathfrak{m}}|S(\alpha)|$. Да вземем произволно $\alpha \in \mathfrak{m}$ и нека τ е определено чрез (17). От лемата на Дирихле (Лема 28) следва, че съществуват $a \in \mathbb{Z}$, $q \in \mathbb{N}$ такива, че

$$\left|\alpha - \frac{a}{q}\right| < \frac{1}{q\tau}, \qquad (a, q) = 1, \qquad q \le \tau. \tag{120}$$

От (20) следва, че $-\frac{1}{\tau} \le \alpha \le 1 - \frac{1}{\tau}$, а първото от трите горни условия е еквивалентно на $\frac{a}{q} - \frac{1}{q\tau} < \alpha < \frac{a}{q} + \frac{1}{q\tau}$. Но тогава имаме

$$-\frac{1}{\tau} < \frac{a}{q} + \frac{1}{q\tau}, \qquad \frac{a}{q} - \frac{1}{q\tau} < 1 - \frac{1}{\tau},$$

или, все едно,

$$-\frac{q+1}{\tau} < a < q - \frac{q-1}{\tau}.$$

От горните неравенства следва, че $-1 \le a \le q - 1$.

Ако предположим, че $a = -1$, то ще имаме $-\frac{q+1}{\tau} < -1$ или, все едно, $\tau - 1 < q$. Оттук и от (17) очевидно следва, че $Q < q$.

Ако пък $0 \le a \le q-1$, то отново ще е изпълнено неравенството $Q < q$. Наистина, да допуснем, че $q \le Q$. Тогава α ще принадлежи на интервал $\left(\frac{a}{q} - \frac{1}{\tau}, \frac{a}{q} + \frac{1}{\tau}\right)$, за който имаме $q \le Q$, $0 \le a \le q - 1$, $(a, q) = 1$. Като си припомним определението (18) за множеството на големите дъги $\mathfrak{M}$, ще направим извода, че $\alpha \in \mathfrak{M}$. Но $\alpha \in \mathfrak{m}$ и получаваме противоречие с (20).

И така, виждаме, че при всички възможни случаи имаме $q > Q$. От друга страна, от $q \le \tau$ следва $\frac{1}{q\tau} \le \frac{1}{q^2}$. Или получихме, че за всяко $\alpha \in \mathfrak{m}$ съществуват $a \in \mathbb{Z}$, $q \in \mathbb{N}$, удовлетворяващи

$$\left|\alpha - \frac{a}{q}\right| < \frac{1}{q^2}, \qquad (a,q) = 1, \qquad Q < q \le \tau. \tag{121}$$

Като приложим Лема 9 и (121), намираме

$$|S(\alpha)| \ll \left(Nq^{-\frac{1}{2}} + N^{\frac{4}{5}} + N^{\frac{1}{2}}q^{\frac{1}{2}}\right)(\log N)^4$$

$$\ll \left(NQ^{-\frac{1}{2}} + N^{\frac{4}{5}} + N^{\frac{1}{2}}\tau^{\frac{1}{2}}\right)(\log N)^4.$$

Последният израз вече не зависи от конкретното $\alpha \in \mathfrak{m}$. Като вземем предвид определенията на Q и τ, дадени в (17), получаваме

$$\sup_{\alpha \in \mathfrak{m}} |S(\alpha)| \ll \frac{N}{(\log N)^{\frac{1}{2}A_1 - 4}} + \frac{N}{(\log N)^{\frac{1}{2}A_2 - 4}}. \tag{122}$$

Това неравенство ни дава възможност да оценим $\mathcal{E}_2$. От (62) и (122) следва

$$\mathcal{E}_2 \ll \frac{N^3}{(\log N)^{A_1 - 9}} + \frac{N^3}{(\log N)^{A_2 - 9}}. \tag{123}$$

2.2.4 Край на доказателството.

Вече оценихме $\mathcal{E}_1$ и $\mathcal{E}_2$. Като използваме (23), (58) и (123), намираме

$$\mathcal{E}(N) \ll \frac{N^3}{(\log N)^{A_1 - 9}} + \frac{N^3}{(\log N)^{2A_2 - 4A_1}} + \frac{N^3}{(\log N)^{A_2 - 9}}.$$

Остава да изберем подходящи стойности за A_1 и A_2, съобразно константата A от формулировката на теоремата. Един възможен избор е $A_1 = A + 10$, $A_2 = 3A + 25$. Той ни дава

$$\mathcal{E}(N) \ll \frac{N^3}{(\log N)^A},$$

с което Теорема 2 е доказана. $\square$

2.3 Тернарният проблем на Голдбах.

В настоящия параграф ще се убедим, че от Теорема 2 сравнително лесно се получава асимптотичната формула на Виноградов, дадена в Теорема 1.

Доказателство на Теорема 1. За величината $R^{(3)}(N)$, зададена чрез (1), използваме определението (4) и получаваме

$$R^{(3)}(N) = \sum_{2<p<N} (\log p) \sum_{p_1+p_2=N-p} (\log p_1)(\log p_2) + O\left(N(\log N)^2\right)$$

$$= \sum_{2<p<N} (\log p)\, R(N-p) + O\left(N(\log N)^2\right). \tag{124}$$

Оттук следва

$$R^{(3)}(N) = H(N) + E(N) + O\left(N(\log N)^2\right), \tag{125}$$

където

$$H\,(N) = \sum_{2<p<N} (\log p)\,(N-p)\,\mathfrak{S}(N-p), \tag{126}$$

$$E(N) = \sum_{2<p<N} (\log p)\,(R(N-p) - (N-p)\mathfrak{S}(N-p)), \tag{127}$$

а самото $\mathfrak{S}(n)$ е зададено чрез (6).

За да оценим $E(N)$, прилагаме последователно неравенството на триъгълника (Лема 29), неравенството на Коши (Лема 30) и Теорема 2. Получаваме, че за произволна константа $A > 0$ е изпълнено

$$E(N) \ll (\log N) \sum_{p<N} |R(N-p) - (N-p)\sigma(N-p)|$$

$$\ll (\log N) \left(\sum_{p<N} 1\right)^{1/2} \left(\sum_{p<N} |R(N-p) - (N-p)\mathfrak{S}(N-p)|^2\right)^{1/2}$$

$$\ll (\log N)\, N^{1/2} \left(\sum_{n\le N} |R(n) - n\mathfrak{S}(n)|^2\right)^{1/2}$$

$$\ll (\log N)\, N^{1/2} \left(\frac{N^3}{(\log N)^{2A+2}}\right)^{1/2}$$

$$\ll \frac{N^2}{(\log N)^A}. \tag{128}$$

И така, виждаме, че от (124), (125) и (128) следва

$$R^{(3)}(N) = H\,(N) + O\left(\frac{N^2}{(\log N)^A}\right). \tag{129}$$

Да разгледаме $H(N)$. За целта, първо ще намерим нов израз за величината $\mathfrak{S}(n)$, определена чрез (6), в случая, когато $2 \mid n$. (Да напомним, че при $2 \nmid n$ имаме $\mathfrak{S}(n) = 0$.) От (6) следва

$$\mathfrak{S}(n) = \prod_{2<p}\left(1 - \frac{1}{(p-1)^2}\right)\prod_{\substack{p|n\\2<p}}\left(1 - \frac{1}{(p-1)^2}\right)^{-1}\prod_{p|n}\left(1 + \frac{1}{p-1}\right)$$

$$= \lambda_0 \prod_{\substack{p|n\\2<p}}\left(1 - \frac{1}{(p-1)^2}\right)^{-1}\prod_{\substack{p|n\\2<p}}\left(1 + \frac{1}{p-1}\right)$$

$$= \lambda_0 \prod_{\substack{p|n\\2<p}}\frac{p-1}{p-2}, \tag{130}$$

където

$$\lambda_0 = 2\prod_{2<p}\left(1 - \frac{1}{(p-1)^2}\right) \tag{131}$$

(очевидно горното произведение е сходящо).

От (130) и (131) получаваме

$$\mathfrak{S}(n) = \lambda_0 \prod_{\substack{p|n\\2<p}}\left(1 + \frac{1}{p-2}\right) = \lambda_0 \sum_{\substack{d|n\\2\nmid d}}\frac{\mu^2(d)}{\varphi_2(d)}, \tag{132}$$

където $\mu(d)$ е функцията на Мьобиус, а $\varphi_2(d)$ е определено чрез

$$\varphi_2(d) = \prod_{p|d}(p-2). \tag{133}$$

Да отбележим, че е в сила оценката

$$\varphi_2(d) \gg \frac{d}{(\log\log(10d))^2} \qquad \text{при} \qquad 2\nmid d, \quad \mu^2(d) = 1. \tag{134}$$

Наистина, според Лема 43 имаме

$$\frac{d}{\varphi(d)} \ll \log\log(10d).$$

От друга страна, ако са изпълнени условията в дясната страна на (134), то като използваме (133) и Лема 42, намираме

$$\frac{\varphi(d)}{\varphi_2(d)} = \frac{d}{\varphi(d)}\prod_{p|d}\left(1 + \frac{1}{p(p-2)}\right) \le \frac{d}{\varphi(d)}\prod_{m=3}^{\infty}\left(1 + \frac{1}{(m-2)^2)}\right) \ll \frac{d}{\varphi(d)}.$$

От последните две формули следва (134).

Ясно е, че при $2 \nmid N$ и $p > 2$ имаме $2 \mid N - p$. Тогава, като използваме (126) и (132), получаваме

$$H(N) = \lambda_0 \sum_{2<p<N} (\log p)(N-p) \sum_{\substack{d \mid (N-p) \\ 2 \nmid d}} \frac{\mu^2(d)}{\varphi_2(d)}.$$

Сега сменяме реда на сумирането и намираме, че

$$H(N) = \lambda_0 \, T(N), \tag{135}$$

където

$$T(N) = \sum_{\substack{d<N \\ 2 \nmid d}} \frac{\mu^2(d)}{\varphi_2(d)} \sum_{\substack{2<p<N \\ p \equiv N \pmod d}} (\log p)(N-p). \tag{136}$$

За да изследваме $T(N)$, разделяме тази сума на две части, съобразно големината на d. Нека $A > 0$ е константата от условието на Теорема 1 и нека

$$D_0 = (\log N)^{A+2}. \tag{137}$$

Имаме

$$T(N) = T_1 + T_2, \tag{138}$$

където

$$T_1 = \sum_{\substack{d \le D_0 \\ 2 \nmid d}} \frac{\mu^2(d)}{\varphi_2(d)} \sum_{\substack{2<p<N \\ p \equiv N \pmod d}} (\log p)(N-p), \tag{139}$$

$$T_2 = \sum_{\substack{D_0<d<N \\ 2 \nmid d}} \frac{\mu^2(d)}{\varphi_2(d)} \sum_{\substack{2<p<N \\ p \equiv N \pmod d}} (\log p)(N-p). \tag{140}$$

Първо ще разгледаме T_2. Сумата по p в (140) очевидно е $\ll N^2(\log N)d^{-1}$. Тогава от (134), (137) и (140) следва

$$T_2 \ll N^2(\log N) \sum_{\substack{D_0<d \le N \\ 2 \nmid d}} \frac{\mu^2(d)}{d\,\varphi_2(d)} \ll N^2(\log N)^2 \sum_{D_0<d \le N} \frac{1}{d^2} \ll \frac{N^2(\log N)^2}{D_0}$$

$$\ll \frac{N^2}{(\log N)^A}. \tag{141}$$

За да изследваме сумата T_1 я представяме във вида

$$T_1 = T_3 + T_4, \tag{142}$$

където

$$T_3 = \sum_{\substack{d\le D_0 \\ (2N,d)=1}} \frac{\mu^2(d)}{\varphi_2(d)} \sum_{\substack{2<p<N \\ p\equiv N \pmod d}} (\log p)(N-p), \tag{143}$$

$$T_4 = \sum_{\substack{d\le D_0 \\ 2\nmid d \\ (N,d)>1}} \frac{\mu^2(d)}{\varphi_2(d)} \sum_{\substack{2<p<N \\ p\equiv N \pmod d}} (\log p)(N-p). \tag{144}$$

За да оценим T_4 ще забележим, че ако $(d,N) = q > 1$, то сумата по p в (144) може да има не повече от едно събираемо (отговарящо на $p = q$). Поради това съображение и от (134) имаме

$$T_4 \ll N(\log N) \sum_{\substack{d<N \\ 2\nmid d}} \frac{\mu^2(d)}{\varphi_2(d)} \ll N(\log N) \sum_{d<N} \frac{\log d}{d} \ll N(\log N)^3. \tag{145}$$

Сега да разгледаме T_3. За целта първо ще се занимаем със сумата по p в (143). Прилагаме преобразованието на Абел (Лема 31) и получаваме

$$\sum_{\substack{2<p\le N \\ p\equiv N \pmod d}} (\log p)(N-p) = \int\limits_0^N \theta(t,d,N)\,dt = \int\limits_{\sqrt{N}}^N \theta(t,d,N)\,dt + O\left(N(\log N)\right),$$

където $\theta(t,d,N)$ е функцията на Чебишев, определена чрез (282). От това равенство и от (134), (143) получаваме

$$T_3 = \sum_{\substack{d\le D_0 \\ (2N,d)=1}} \frac{\mu^2(d)}{\varphi_2(d)} \int\limits_{\sqrt{N}}^N \theta(t,d,N)\,dt + O\left(N(\log N)^3\right).$$

Заместваме в горната формула $\theta(t,d,N)$ с израза, който ни дава теоремата на Зигел (Лема 54). Да отбележим, че условието $d \le (\log t)^D$, където $D > 0$ е константа, е налице, тъй като $t \in [\sqrt{N}, N]$. Използваме също (134) и получаваме

$$T_3 = \sum_{\substack{d \le D_0 \\ (2N,d)=1}} \frac{\mu^2(d)}{\varphi_2(d)} \int\limits_{\sqrt{N}}^{N} \left(\frac{t}{\varphi(d)} + O\left(N e^{-c\sqrt{\log N}} \right) \right) dt + O\left(N (\log N)^3 \right)$$

$$= \sum_{\substack{d \le D_0 \\ (2N,d)=1}} \frac{\mu^2(d)}{\varphi(d)\,\varphi_2(d)} \int\limits_{\sqrt{N}}^{N} t\, dt + O\left(N^2 e^{-c\sqrt{\log N}} \sum_{\substack{d \le D_0 \\ (2N,d)=1}} \frac{\mu^2(d)}{\varphi_2(d)} \right)$$

$$= \frac{N^2}{2} \sum_{\substack{d \le D_0 \\ (2N,d)=1}} \frac{\mu^2(d)}{\varphi(d)\,\varphi_2(d)} + O\left(\frac{N^2}{(\log N)^A} \right). \tag{146}$$

От (129), (135), (138), (141), (142), (145) и (146) получаваме

$$R^{(3)}(N) = \lambda_0 \, \frac{N^2}{2} \sum_{\substack{d \le D_0 \\ (2N,d)=1}} \frac{\mu^2(d)}{\varphi(d)\,\varphi_2(d)} + O\left(\frac{N^2}{(\log N)^A} \right). \tag{147}$$

Следващата стъпка е да заместим сумата по d със съответния безкраен ред

$$\mathcal{F}(N) = \sum_{\substack{d=1 \\ (2N,d)=1}}^{\infty} \frac{\mu^2(d)}{\varphi(d)\,\varphi_2(d)}. \tag{148}$$

Тогава вместо (147) получаваме

$$R^{(3)}(N) = \lambda_0 \, \mathcal{F}(N) \, \frac{N^2}{2} + O\left(N^2 \sum_{\substack{d > D_0 \\ 2 \nmid d}} \frac{\mu^2(d)}{\varphi(d)\,\varphi_2(d)} \right) + O\left(\frac{N^2}{(\log N)^A} \right). \tag{149}$$

Но от (134), (137) и Лема 43 имаме

$$\sum_{\substack{d > D_0 \\ 2 \nmid d}} \frac{\mu^2(d)}{\varphi(d)\,\varphi_2(d)} \ll \sum_{d > D_0} \frac{(\log\log(10d))}{d^2} \ll \frac{\log N}{D_0} = (\log N)^{-A-1},$$

следователно първият остатъчен член в (149) може да бъде пропуснат. Получаваме

$$R^{(3)}(N) = \lambda_0 \, \mathcal{F}(N) \, \frac{N^2}{2} + O\left(\frac{N^2}{(\log N)^A} \right). \tag{150}$$

Остава да се убедим, че

$$\lambda_0 \, \mathcal{F}(N) = \mathfrak{S}^{(3)}(N), \tag{151}$$

и Теорема 1 ще бъде доказана. За тази цел към сумата $\mathcal{F}(N)$, зададена чрез (148), прилагаме тъждеството на Ойлер (Лема 35) и, като използваме (131), (133), (148) и Лема 42, получаваме последователно

$$
\begin{aligned}
\lambda_0\,\mathcal{F}(N) &= 2\prod_{p>2}\left(1-\frac{1}{(p-1)^2}\right)\prod_{p\nmid 2N}\left(1+\frac{1}{(p-2)(p-1)}\right) \\
&= 2\prod_{p>2}\left(1-\frac{1}{(p-1)^2}\right)\prod_{p>2}\left(1+\frac{1}{(p-2)(p-1)}\right)\prod_{p\mid N}\left(1+\frac{1}{(p-2)(p-1)}\right)^{-1} \\
&= 2\prod_{p>2}\left[\left(1-\frac{1}{(p-1)^2}\right)\left(1+\frac{1}{(p-2)(p-1)}\right)\right]\prod_{p\mid N}\left(1+\frac{1}{(p-2)(p-1)}\right)^{-1} \\
&= \prod_{p}\left(1+\frac{1}{(p-1)^3}\right)\prod_{p\mid N}\frac{(p-1)(p-2)}{p^2-3p+3} \\
&= \prod_{p\nmid N}\left(1+\frac{1}{(p-1)^3}\right)\prod_{p\mid N}\left[\left(1+\frac{1}{(p-1)^3}\right)\frac{(p-1)(p-2)}{p^2-3p+3}\right] \\
&= \prod_{p\nmid N}\left(1+\frac{1}{(p-1)^3}\right)\prod_{p\mid N}\frac{p(p-2)}{(p-1)^2} \\
&= \prod_{p\nmid N}\left(1+\frac{1}{(p-1)^3}\right)\prod_{p\mid N}\left(1-\frac{1}{(p-1)^2}\right).
\end{aligned}
$$

Като вземем предвид последната формула и определението (3), виждаме, че е изпълнено (151). С това Теорема 1 е доказана. □

3 Проблем на Варинг

3.1 Увод и формулировка на теоремата

Да означим с $I_{k,n}(N)$ броя на k-торките естествени числа $x_1, \ldots, x_k$, за които е изпълнено

$$x_1^n + \cdots + x_k^n = N \tag{152}$$

в естествени числа $x_1, \ldots, x_k$. Ще докажем на следната

Теорема 10. *Нека*

$$n \geq 2, \qquad\qquad k \geq 2^n + 1. \tag{153}$$

Съществуват

$$\delta = \delta(k,n) > 0, \qquad c_1 = c_1(k,n) > 0, \qquad c_2 = c_2(k,n) > 0$$

независещи от N и такива, че е в сила асимптотичната формула

$$I_{k,n}(N) = \frac{\Gamma\left(1+\frac{1}{n}\right)^k}{\Gamma\left(\frac{k}{n}\right)} \mathfrak{S}_{k,n}(N)\, N^{\frac{k}{n}-1} + O\left(N^{\frac{k}{n}-1-\delta}\right), \tag{154}$$

където

$$c_1 \leq \mathfrak{S}_{k,n}(N) \leq c_2 \tag{155}$$

и $\Gamma(t)$ е гама-функцията на Ойлер.

От горната асимптотична формула следва, че ако са налице условията (153), то съществува $N_0 = N_0(k,n) > 0$ такова, че при $N \geq N_0(k,n)$ е изпълнено $I_{k,n}(N) > 0$, т.е. уравнението (152) е разрешимо в естествени числа $x_1, \ldots, x_k$.

3.2 Доказателство на Теорема 10.

3.2.1 Начало на доказателството.

Полагаме

$$P = N^{\frac{1}{n}}. \tag{156}$$

Като използваме Лема 27 записваме $I_{k,n}(N)$ във вида

$$I_{k,n}(N) = \sum_{\substack{x_1,\dots,x_k \le P \\ x_1^n+\dots+x_k^n=N}} 1$$

$$= \sum_{x_1,\dots,x_k \le P} \int\limits_0^1 e\left(\alpha\left(x_1^n + \dots + x_k^n - N\right)\right) d\alpha$$

$$= \int\limits_0^1 \sum_{x_1,\dots,x_k \le P} e\left(\alpha\left(x_1^n + \dots + x_k^n - N\right)\right) d\alpha$$

$$= \int\limits_0^1 V(\alpha)^k e\left(-\alpha N\right) d\alpha, \tag{157}$$

където

$$V(\alpha) = \sum_{x \le P} e\left(\alpha x^n\right). \tag{158}$$

Полагаме

$$Q = P^{\frac{1}{100}}, \qquad \tau = P^n Q^{-1} \tag{159}$$

и определяме множествата на големите и на малките дъги чрез формулите

$$\mathfrak{M} = \bigcup_{q \le Q} \bigcup_{\substack{a=0 \\ (a,q)=1}}^{q-1} \left[\frac{a}{q} - \frac{1}{q\tau}, \frac{a}{q} + \frac{1}{q\tau}\right], \tag{160}$$

$$\mathfrak{m} = \left[-\frac{1}{\tau}, 1 - \frac{1}{\tau}\right] \setminus \mathfrak{M}. \tag{161}$$

Тогава от (157) получаваме

$$I_{k,n}(N) = I' + I'', \tag{162}$$

където

$$I' = \int\limits_{\mathfrak{M}} V(\alpha)^k e\left(-\alpha N\right) d\alpha, \qquad I'' = \int\limits_{\mathfrak{m}} V(\alpha)^k e\left(-\alpha N\right) d\alpha. \tag{163}$$

3.2.2 Оценка на I''.

Експоненциални суми и крайни разлики. Нека е дадена функцията $f : \mathbb{R} \to \mathbb{R}$ и числата $h_1, \dots, h_s \in \mathbb{R}$. Определяме $\Delta_{h_1,\dots,h_s} f(x)$ чрез формулите

$$\Delta_{h_1} f(x) = f(x + h_1) - f(x),$$

$$\Delta_{h_1,\dots,h_s} f(x) = \Delta_{h_1,\dots,h_{s-1}}\left(\Delta_{h_s} f(x)\right).$$

Изпълнена е следната елементарна

Лема 11. *Величината* $\Delta_{h_1,\ldots,h_s} f(x)$ *не зависи от реда на променливите* $h_1, \ldots, h_s$.

Доказателство: При $s = 2$ се проверява непосредствено, че

$$\Delta_{h_1,h_2} f(x) = f(x + h_1 + h_2) - f(x + h_1) - f(x + h_2) + f(x).$$

Предоставяме на читателя да докаже твърдението в общия случай, като използва математическа индукция. □

Лема 12. *Нека*

$$f(x) = \alpha_0 x^s + \alpha_1 x^{s-1} + \cdots + \alpha_s$$

е полином с реални коефициенти от степен $s \geq 2$. *Тогава за произволни* $h_1, \ldots, h_{s-1} \in \mathbb{R}$ *е изпълнено*

$$\Delta_{h_1,\ldots h_{s-1}} f(x) = s!\, \alpha_0\, h_1 \ldots h_{s-1}\, x + \beta,$$

където β *не зависи от* x.

Доказателство: Имаме

$$\Delta_h f(x) = \alpha_0 (x+h)^2 + \alpha_1 (x+h) + \alpha_2 - \alpha_0 x^2 - \alpha_1 x - \alpha_2 = 2\,\alpha_0\, h\, x + \alpha_0 h^2 + \alpha_1 h,$$

следователно при $s = 2$ твърдението е вярно. Да допуснем, че твърдението е вярно при някое $s \geq 2$. Нека е даден полиномът

$$F(x) = \alpha_0 x^{s+1} + \alpha_1 x^s + \cdots + \alpha_{s+1}$$

и нека $h_1, \ldots, h_s \in \mathbb{R}$. Ясно е, че

$$\Delta_{h_s} F(x) = F(x + h_s) - F(x) = (s+1)\,\alpha_0\, h_s\, x^s + \alpha_1' x^{s-1} + \cdots + \alpha_s',$$

където коефициентите α_j' не зависят от x. Тогава, като използваме индукционното предположение, получаваме

$$\Delta_{h_1,\ldots,h_s} F(x) = \Delta_{h_1,\ldots,h_{s-1}} \left(\Delta_{h_s} F(x)\right) = s!\,(s+1)\,\alpha_0\, h_s\, h_1 \ldots h_{s-1}\, x + \beta$$

$$= (s+1)!\,\alpha_0\, h_1 \ldots h_s\, x + \beta,$$

където β не зависи от x. С това лемата е доказана. □

Лема 13. *Нека* $n \geq 2$ *и нека* $h_1, \ldots, h_s \in \mathbb{R}$ *са произволни, като* $s \leq n$. *Тогава*

$$\Delta_{h_1,\ldots,h_s} x^n = h_1 \ldots h_s \Phi(x, h_1, \ldots, h_s),$$

където $\Phi(x, h_1, \ldots, h_s) \in \mathbb{Z}[x, h_1, \ldots, h_s]$. *Степента на* Φ *относно* x *е равна на* $n - s$ *и коефициентът му пред* x^{n-s} *не зависи от* $h_1, \ldots, h_s$. *Степента на* Φ *относно коя да е от променливите* h_j *не надминава* n.

Доказателство: Получава се по индукция — оставяме простите разсъждения на читателя. $\square$

Лема 14. *Нека $P \in \mathbb{R}$, $P \geq 1$, нека е дадена функцията $f : [1, P] \to \mathbb{R}$ и нека*

$$V = \sum_{x \leq P} e\left(f(x)\right).$$

За всяко $l \in \mathbb{N}$ е изпълнено неравенството

$$|V|^{2^l} \leq (3P)^{2^l - l - 1} \sum_{|h_1| < P} \cdots \sum_{|h_l| < P} \sum_{x \in I_{h_1, \ldots h_l}} e\left(\Delta_{h_1, \ldots, h_l} f(x)\right), \tag{164}$$

където $I_{h_1, \ldots, h_l}$ са подинтервали на $[1, P]$, определени индуктивно по следния начин:

$$I_{h_1} = [1, P] \cap [1 - h_1, P - h_1],$$

$$I_{h_1, \ldots, h_s} = \{\alpha \in I_{h_1, \ldots, h_{s-1}} \ : \ \alpha + h_s \in I_{h_1, \ldots, h_{s-1}}\}.$$

Доказателство: Имаме

$$|V|^2 = V\,\overline{V} = \sum_{y \leq P} e\left(f(y)\right) \sum_{x \leq P} e\left(-f(x)\right) \ = \sum_{x,\, y \leq P} e\left(f(y) - f(x)\right).$$

Разделяме последната сума на части съобразно стойността на разликата $y - x$ и получаваме

$$|V|^2 = \sum_{|h| < P} \sum_{\substack{x,\, y \leq P \\ y - x = h}} e\left(f(y) - f(x)\right)$$

$$= \sum_{|h| < P} \sum_{\substack{1 \leq x \leq P \\ 1 \leq x + h \leq P}} e(f(x + h) - f(x))$$

$$= \sum_{|h| < P} \sum_{x \in I_h} e\left(\Delta_h f(x)\right).$$

Или при $l = 1$ твърдението е доказано.

Нека допуснем, че (164) е изпълнено при някое l. Тогава от неравенството на триъгълника (Лема 29) следва

$$|V|^{2^l} \leq (3P)^{2^l - l - 1} \Sigma, \tag{165}$$

където

$$\Sigma = \sum_{|h_1| < P} \cdots \sum_{|h_l| < P} |\mathcal{H}_{h_1, \ldots, h_l}|,$$

$$\mathcal{H} = \mathcal{H}_{h_1, \ldots, h_l} = \sum_{x \in I_{h_1, \ldots, h_l}} e\left(\Delta_{h_1, \ldots, h_l} f(x)\right). \tag{166}$$

Като използваме (165) и неравенството на Коши (Лема 30) получаваме

$$|V|^{2^{l+1}} = \left(|V|^{2^l}\right)^2 \le \left((3P)^{2^l-l-1}\right)^2 \Sigma^2 = (3P)^{2^{l+1}-2l-2}\,\Sigma^2$$

$$\le (3P)^{2^{l+1}-2l-2}\,\Sigma'\,\Sigma'', \tag{167}$$

където

$$\Sigma' = \sum_{|h_1|<P} \cdots \sum_{|h_l|<P} 1, \qquad \Sigma'' = \sum_{|h_1|<P} \cdots \sum_{|h_l|<P} |\mathcal{H}_{h_1,\dots,h_l}|^2. \tag{168}$$

Очевидно имаме $|\Sigma'| \le (3P)^l$ и като вземем предвид (167) получаваме

$$|V|^{2^{l+1}} \le (3P)^{2^{l+1}-l-2}\,\Sigma''. \tag{169}$$

Да разгледаме Σ''. От (166) следва

$$|\mathcal{H}|^2 = \mathcal{H}\,\overline{\mathcal{H}} = \sum_{x\in I_{h_1,\dots,h_l}} \sum_{y\in I_{h_1,\dots,h_l}} e\left(\Delta_{h_1,\dots,h_l} f(y) - \Delta_{h_1,\dots,h_l} f(x)\right).$$

Разделяме последната сума на части съобразно стойността на разликата $y - x$ и получаваме

$$|\mathcal{H}|^2 = \sum_{|h|<P} \sum_{\substack{x\in I_{h_1,\dots,h_l}\\ x+h\in I_{h_1,\dots,h_l}}} e\left(\Delta_{h_1,\dots,h_l} f(x+h) - \Delta_{h_1,\dots,h_l} f(x)\right)$$

$$= \sum_{|h_{l+1}|<P} \sum_{x\in I_{h_1,\dots,h_{l+1}}} e\left(\Delta_{h_1,\dots,h_{l+1}} f(x)\right). \tag{170}$$

От (168), (169) и (170) следва

$$|V|^{2^{l+1}} \le (3P)^{2^{l+1}-(l+1)-1} \sum_{|h_1|<P} \cdots \sum_{|h_{l+1}|<P} \sum_{x\in I_{h_1,\dots,h_{l+1}}} e\left(\Delta_{h_1,\dots,h_{l+1}} f(x)\right).$$

Индукционната стъпка е извършена, с което лемата е доказана. □

Оценка на експоненциална сума по метода на Херман Вайл.

Лема 15. *Нека е даден полиномът* $f(x) = \alpha_0 x^s + \alpha_1 x^{s-1} + \cdots + \alpha_s$ *от степен* $s \ge 2$*, нека* $P \in \mathbb{R}$, $P \ge 1$ *и*

$$V = \sum_{x\le P} e\left(f(x)\right).$$

Ако съществуват $a \in \mathbb{Z}$, $q \in \mathbb{N}$*, такива че*

$$\left|\alpha_0 - \frac{a}{q}\right| \le \frac{1}{q^2}, \qquad (a,q) = 1, \tag{171}$$

то за произволно $\varepsilon > 0$ *е в сила оценката*

$$|V| \ll P^{1+\varepsilon} \left(\frac{1}{q} + \frac{1}{P} + \frac{q}{P^s}\right)^{\frac{1}{2^{s-1}}}. \tag{172}$$

Константата в знака на Виноградов в (172) *зависи само от* s *и* ε*.*

Доказателство. Можем да считаме, че

$$q \le P^s, \tag{173}$$

тъй като в противен случай (172) е следствие от тривиалната оценка $|V| \le P$.

Прилагаме Лема 14 при $l = s - 1$ и получаваме

$$|V|^{2^{s-1}} \ll P^{2^{s-1}-(s-1)-1} \sum_{|h_1|<P} \cdots \sum_{|h_{s-1}|<P} |\mathcal{H}|, \tag{174}$$

където

$$\mathcal{H} = \mathcal{H}_{h_1,\dots,h_{s-1}} = \sum_{x \in I_{h_1,\dots,h_{s-1}}} e\left(\Delta_{h_1,\dots,h_{s-1}} f(x)\right), \tag{175}$$

а $I_{h_1,\dots,h_{s-1}}$ е подинтервал на $[1, P]$. От (174) следва

$$|V|^{2^{s-1}} \ll P^{2^{s-1}-s} \left(\Sigma' + \Sigma''\right), \tag{176}$$

където Σ' съдържа събираемите, за които $h_j = 0$ за някое j, а Σ'' е съставена от събираемите, за които $h_j \ne 0$ за всички j.

Да разгледаме първо Σ'. Като използваме тривиалната оценка $|\mathcal{H}| \le P$ и определението на Σ' намираме

$$\Sigma' \ll P^{s-1}. \tag{177}$$

Сега да оценим Σ''. От Лема 12 следва, че

$$\Delta_{h_1,\dots,h_{s-1}} f(x) = s!\, \alpha_0\, h_1 \dots h_{s-1}\, x + \beta,$$

където β не зависи от x. Тогава, като се възползваме от Лема 5 виждаме, че за сумата $\mathcal{H}$, определена чрез (175), е изпълнено

$$|\mathcal{H}| = \left| \sum_{x \in I_{h_1,\dots,h_{s-1}}} e(s!\, \alpha_0\, h_1 \dots h_{s-1}\, x) \right| \le \min\left(P, ||s!\, \alpha_0\, h_1 \dots h_{s-1}||^{-1}\right).$$

От горното неравенство и от определението на Σ'' следва

$$\Sigma'' \ll \sum_{0<|h_1|<P} \cdots \sum_{0<|h_{s-1}|<P} \min\left(P, ||s!\, \alpha_0\, h_1 \dots h_{s-1}||^{-1}\right).$$

Последната сума не се променя, ако сумираме само по положителните стойности на h_j и я умножим по 2^{s-1}. Тъй като считаме, че константата в знака на Виноградов в (172) зависи от s, то можем да запишем

$$\Sigma'' \ll \sum_{h_1<P} \cdots \sum_{h_{s-1}<P} \min\left(P, ||s!\, \alpha_0\, h_1 \dots h_{s-1}||^{-1}\right),$$

като сумирането е вече само по положителни h_j. Разделяме последната сума на части съобразно стойността на израза $s!h_1 \dots h_{s-1}$ и получаваме

$$\Sigma'' \ll \sum_{m \leq s!\, P^{s-1}} \kappa(m)\ \min\left(P, ||\alpha_0\, m||^{-1}\right),$$

където $\kappa(m)$ е броят на решенията на уравнението

$$s!\, h_1 \dots h_{s-1} = m$$

в естествени числа $h_1, \dots, h_{s-1}$. Очевидно $\kappa(m) \leq \tau^{s-1}(m)$ и, като се възползваме от Лема 37, получаваме

$$\Sigma'' \ll P^{\varepsilon}\, \Sigma^*, \tag{178}$$

където

$$\Sigma^* = \sum_{m \leq s!\, P^{s-1}} \min\left(P, ||\alpha_0\, m||^{-1}\right).$$

Последната сума оценяваме с помощта на Лема 8. Като използваме условието (171), намираме

$$\Sigma^* \ll \sum_{m \leq s!\, P^{s-1}} \min\left(\frac{s!P^{s-1} \cdot P}{m}, ||\alpha_0\, m||^{-1}\right) \ll P^{s+\varepsilon}\ \left(\frac{1}{q} + \frac{1}{P} + \frac{q}{P^s}\right). \tag{179}$$

Като се възползваме от (178) и (179) и предефинираме ε, получаваме

$$\Sigma'' \ll P^{s+\varepsilon}\ \left(\frac{1}{q} + \frac{1}{P} + \frac{q}{P^s}\right). \tag{180}$$

От оценките (176), (177) и (180) следва

$$|V|^{2^{s-1}} \ll P^{2^{s-1}+\varepsilon}\ \left(\frac{1}{q} + \frac{1}{P} + \frac{q}{P^s}\right)$$

Повдигаме двете страни на последното неравенство в степен $\frac{1}{2^{s-1}}$ и, след като отново предефинираме ε, получаваме (172). С това лемата е доказана. $\square$

Неравенство на Хуа

Лема 16. *Нека $P \in \mathbb{R}$, $P \geq 1$, $n \in \mathbb{N}$ и*

$$V(\alpha) = \sum_{x \leq P} e\left(\alpha x^n\right). \tag{181}$$

Тогава за всяко $s = 1, 2, \dots, n$ и за произволно малко $\varepsilon > 0$ е изпълнено

$$\int_0^1 |V(\alpha)|^{2^s}\, d\alpha \ll P^{2^s - s + \varepsilon}, \tag{182}$$

като константата в знака на Виноградов зависи само от n и ε.

Доказателство. Ще докажем твърдението с помощта на индукция по s. Като използваме Лема 27 получаваме

$$\int_0^1 |V(\alpha)|^2 \, d\alpha = \int_0^1 V(\alpha)V(-\alpha) \, d\alpha = \int_0^1 \sum_{x,\, y \le P} e\left(\alpha\left(x^n - y^n\right)\right) \, d\alpha$$

$$= \sum_{x,\, y \le P} \int_0^1 e\left(\alpha\left(x^n - y^n\right)\right) \, d\alpha = \sum_{x \le P} 1 \le P.$$

Следователно при $s = 1$ неравенството (182) е изпълнено. Тогава при $n = 1$ твърдението е вярно и оттук нататък ще предполагаме, че $n \ge 2$.

Да допуснем, че (182) е вярно за някое естествено число $s \le n - 1$. Полагаме за простото на записа $2^{s-1} = t$. Тогава, като използваме (181), получаваме

$$|V(\alpha)|^{2^s} = |V(\alpha)|^{2t} = V(\alpha)^t V(-\alpha)^t$$

$$= \sum_{x_1, y_1, \dots, x_t, y_t \le P} e\left(\alpha\left(x_1^n + \cdots + x_t^n - y_1^n - \cdots - y_t^n\right)\right). \tag{183}$$

За произволно $h \in \mathbb{Z}$ да означим с b_h броя на решенията на уравнението

$$y_1^n + \cdots + y_t^n - x_1^n - \cdots - x_t^n = h \tag{184}$$

в естествени числа, удовлетворяващи

$$x_1, y_1, \dots x_t, y_t \le P. \tag{185}$$

Тогава от (183) получаваме

$$|V(\alpha)|^{2^s} = \sum_{h \in \mathbb{Z}} b_h \, e(-\alpha h). \tag{186}$$

Преди да продължим по-нататък, ще изредим някои от свойствата на числата b_h. Очевидно

$$b_h \ge 0 \qquad \text{за всяко} \qquad h \in \mathbb{Z}. \tag{187}$$

От (184) и (185) следва

$$b_h = 0 \qquad \text{при} \qquad |h| > t\,P^n, \tag{188}$$

така че безкрайният ред в (186) всъщност е крайна сума.

От определението на b_h се вижда, че сумата $\sum_{h \in \mathbb{Z}} b_h$ е равна на броя на всички набори естествени числа, удовлетворяващи (185). Следователно

$$\sum_{h \in \mathbb{Z}} b_h \le P^{2t} = P^{2^s}. \tag{189}$$

Накрая, в сила е оценката

$$b_0 \ll P^{2^s - s + \varepsilon}. \tag{190}$$

Наистина, ако интегрираме почленно равенството (186) и използваме Лема 27, получаваме

$$b_0 = \int_0^1 |V(\alpha)|^{2^s} \, d\alpha.$$

Тогава (190) е следствие от индукционното предположение.

Да продължим с доказателството. От Лема 14 при $f(x) = \alpha x^n$ получаваме

$$|V(\alpha)|^{2^s} \leq (3P)^{2^s - s - 1} \sum_{|h_1| < P} \cdots \sum_{|h_s| < P} \sum_{x \in I_{h_1, \ldots, h_s}} e\left(\Delta_{h_1, \ldots, h_s}\left(\alpha x^n\right)\right), \tag{191}$$

където $I_{h_1, \ldots, h_s}$ е подинтервал на $[1, P]$. По-нататък, от Лема 13 следва, че

$$\Delta_{h_1, \ldots, h_s}\left(\alpha x^n\right) = \alpha \Delta_{h_1, \ldots, h_s}\left(x^n\right) = \alpha \, h_1 \ldots h_s \, \Phi(x, h_1, \ldots, h_s), \tag{192}$$

където $\Phi(x, h_1, \ldots, h_s) \in \mathbb{Z}[x, h_1, \ldots, h_s]$. Степента на Φ относно x е равна на $n - s$ и коефициентът му пред x^{n-s} не зависи от $h_1, \ldots, h_s$. Оттук следва, че при фиксирани $d, h_1, \ldots, h_s \in \mathbb{Z}$ уравнението

$$\Phi(x, h_1, \ldots, h_s) = d$$

притежава не повече от n решения относно x.

За произволно $h \in \mathbb{Z}$ означаваме с c_h броя на решенията на уравнението

$$h_1 \ldots h_s \, \Phi(x, h_1, \ldots h_s) = h \tag{193}$$

в цели числа $x, h_1, \ldots, h_s$, удовлетворяващи условията

$$|h_1| < P, \ldots, |h_s| < P, \qquad x \in I_{h_1, \ldots, h_s}. \tag{194}$$

Тогава от (191) следва

$$|V(\alpha)|^{2^s} \leq (3P)^{2^s - s - 1} \sum_{h \in \mathbb{Z}} c_h \, e(\alpha h). \tag{195}$$

Сега ще изредим някои от свойствата на числата c_h. От определението им и от свойствата на полинома Φ се вижда, че съществуват $\omega, \omega_1 > 0$, зависещи само от n и такива, че

$$c_h = 0 \qquad \text{при} \qquad |h| > \omega_1 P^{\omega}. \tag{196}$$

По-нататък, изпълнено е

$$c_0 \ll P^s, \tag{197}$$

като константата в знака на Виноградов зависи от n. Наистина, c_0 е равно на броя на решенията на уравнението

$$h_1 \ldots h_s \, \Phi(x, h_1, \ldots . h_s) = 0 \tag{198}$$

в цели числа, удовлетворяващи (194). Ако е изпълнено (198) има две възможности:

1) Някое h_j е равно на нула. Тогава това h_j е фиксирано, а всяко от останалите h_ν, $\nu \neq j$, както и x приемат не повече от $O(P)$ стойности.

2) Всички h_j са различни от нула. Тогава всяко от тях приема не повече от $O(P)$ стойности. Освен това, от (193) следва, че $\Phi(x, h_1, \ldots, h_s) = 0$, следователно x може да приема не повече от n стойности.

От изложените разсъждения следва оценката (197).

Накрая ще отбележим, че за произволно малко $\varepsilon > 0$ имаме

$$c_h \ll P^\varepsilon \qquad \text{при} \qquad h \neq 0. \tag{199}$$

Наистина, ако $h \neq 0$ и е налице (193), то всяко h_j е делител на h, следователно може да приема най-много $2\tau(|h|)$ стойности. При фиксирани h_j променливата x може да приема най-много n стойности, тъй като е корен на уравнението

$$\Phi(x, h_1, \ldots, h_s) = h(h_1 \ldots h_s)^{-1}.$$

Следователно при $h \neq 0$ имаме $c_h \leq n\, 2^n \, \tau(|h|)^n$. От последното неравенство и от Лема 37 следва, че (199) е изпълнено при $0 < |h| \leq \omega_1 P^\omega$.

Ако пък $|h| > \omega_1 P^\omega$, то (199) е тривиално следствие от (196).

Сега вече можем да завършим доказателството на лемата. Като използваме (186), (195) и Лема 27, получаваме

$$\begin{aligned}
\int_0^1 |V(\alpha)|^{2^{s+1}} \, d\alpha &= \int_0^1 |V(\alpha)|^{2^s} \cdot |V(\alpha)|^{2^s} \, d\alpha \\
&\leq \int_0^1 (3P)^{2^s - s - 1} \sum_{m \in \mathbb{Z}} c_m \, e(\alpha m) \sum_{h \in \mathbb{Z}} b_h \, e(-\alpha h) \, d\alpha \\
&= (3P)^{2^s - s - 1} \sum_{h,\, m \in \mathbb{Z}} c_m b_h \int_0^1 e(\alpha(m - h)) \, d\alpha \\
&= (3P)^{2^s - s - 1} \sum_{h \in \mathbb{Z}} b_h \, c_h.
\end{aligned} \tag{200}$$

По-нататък, от (187), (188), (189), (190), (197) и (199) последователно намираме

$$\begin{aligned}\sum_{h\in\mathbb{Z}} b_h\, c_h &= b_0\, c_0 + \sum_{\substack{h\in\mathbb{Z}\\ h\neq 0}} b_h\, c_h \\ &\ll P^{2^s-s+\varepsilon} P^s + P^{\varepsilon} \sum_{\substack{h\in\mathbb{Z}\\ h\neq 0}} b_h \\ &\ll P^{2^s+\varepsilon} + P^{\varepsilon} \sum_{h\in\mathbb{Z}} b_h \\ &\ll P^{2^s+\varepsilon}. \qquad (201)\end{aligned}$$

Сега от (200) и (201) следва

$$\int\limits_0^1 |V(\alpha)|^{2^{s+1}}\, d\alpha \ll P^{2\cdot 2^s-(s+1)+\varepsilon} = P^{2^{s+1}-(s+1)+\varepsilon}.$$

С това индукционната стъпка е извършена и лемата е доказана. □

Завършване на оценката на I''. Като използваме (153) и (163) получаваме

$$|I''| \le \int\limits_{\mathfrak{m}} |V(\alpha)|^k\, d\alpha \le \left(\sup_{\alpha\in\mathfrak{m}} |V(\alpha)|\right)^{k-2^n} \int\limits_{\mathfrak{m}} |V(\alpha)|^{2^n}\, d\alpha. \qquad (202)$$

Като разсъждаваме точно както при оценяването на сумата $S(\alpha)$ при изследването на проблема на Голдбах[1], установяваме, че ако $\alpha\in\mathfrak{m}$, където $\mathfrak{m}$ е множеството на малките дъги, определено чрез (160), то съществуват $a, q\in\mathbb{Z}$ такива, че

$$\left|\alpha - \frac{a}{q}\right| \le \frac{1}{q^2}, \qquad (a,q)=1, \qquad Q < q \le \tau, \qquad (203)$$

като Q и τ са определени чрез (159). Но тогава от Лема 15 следва, че

$$\sup_{\alpha\in\mathfrak{m}} |V(\alpha)| \ll P^{1+\varepsilon}\left(\frac{1}{Q} + \frac{1}{P} + \frac{\tau}{P^n}\right)^{\frac{1}{2^{n-1}}} \ll P^{1-\frac{1}{100\cdot 2^{n-1}}+\varepsilon} \ll P^{1-\frac{1}{100\cdot 2^n}}. \qquad (204)$$

От друга страна, от Лема 16 намираме

$$\int\limits_{\mathfrak{m}} |V(\alpha)|^{2^n}\, d\alpha \le \int\limits_0^1 |V(\alpha)|^{2^n}\, d\alpha \ll P^{2^n-n+\varepsilon}. \qquad (205)$$

[1] Виж параграфа, включващ формула (121).

От (202), (204) и (205) получаваме

$$|I''| \ll P^{(k-2^n)\left(1-\frac{1}{100\cdot 2^n}\right)} P^{2^n-n+\varepsilon} \ll P^{k-n-\frac{1}{200\cdot 2^n}}.$$

От горната оценка и от (156) следва

$$|I''| \ll N^{\frac{k}{n}-1-\delta_1}, \qquad \delta_1 = \frac{1}{200\, n\, 2^n}. \tag{206}$$

3.2.3 Асимптотична формула за I'.

Никои два от интервалите, съставящи големите дъги, не се пресичат. За да се покаже това се разръждава както в началото на параграф 2.2.2 от настоящите записки. Следователно, като използваме (160) и (163) и извършим смяна на променливата в интеграла, получаваме

$$I' = \sum_{q \le Q} \sum_{\substack{a=0 \\ (a,q)=1}}^{q-1} \int\limits_{-1/(q\tau)}^{1/(q\tau)} V^k\left(\frac{a}{q}+\beta\right) e\left(-N\left(\frac{a}{q}+\beta\right)\right) d\beta \tag{207}$$

За да продължим по-нататък ще докажем следната

Лема 17. *Ако са изпълнени условията*

$$q \le Q, \qquad |\beta| \le \frac{1}{q\tau}, \qquad (a,q)=1, \tag{208}$$

то за сумата $V(\alpha)$, определена чрез (158), е в сила асимптотичната формула:

$$V\left(\frac{a}{q}+\beta\right) = \frac{S(q,a)}{q} W(\beta) + O\left(q(1+N|\beta|)\right), \tag{209}$$

където

$$W(\beta) = \frac{1}{n} \sum_{m=1}^{N} e(\beta m)\, m^{\frac{1}{n}-1}, \tag{210}$$

$$S(q,a) = \sum_{x=1}^{q} e\left(\frac{a}{q}x^n\right) \tag{211}$$

Доказателство. Прилагаме (158), Лема 27 и преобразованието на Абел (Лема 31). Получаваме

$$V\left(\frac{a}{q}+\beta\right) = \sum_{\substack{x\in\mathbb{N} \\ x^n \le N}} e\left(\frac{a}{q}x^n\right) e(\beta x^n) = -\int\limits_0^N H\left(t^{\frac{1}{n}}\right) \frac{d}{dt} e(\beta t)\, dt + H(P)\, e(\beta N), \tag{212}$$

където
$$H(u)=\sum_{x\le u} e\left(\frac{a}{q}x^n\right). \tag{213}$$

За да изследваме $H(u)$, разделяме тази сума на части според остатъка на x по модул q. След това използваме Лема 27 и очевидния факт, че броят на числата по-малки или равни на u, даващи един и същи остатък по модул q, е равен на $u/q+O(1)$. Получаваме

$$H(u)=\sum_{m=1}^{q}\sum_{\substack{x\le u\\ x\equiv m \pmod q}} e\left(\frac{a}{q}x^n\right)=\sum_{m=1}^{q} e\left(\frac{a}{q}m^n\right)\sum_{\substack{x\le u\\ x\equiv m \pmod q}} 1$$

$$=\frac{S(q,a)}{q}u+O(q). \tag{214}$$

Заместваме този израз в (212) и намираме

$$V\left(\frac{a}{q}+\beta\right)=-\int\limits_0^N \left(\frac{S(q,a)}{q}\,t^{\frac{1}{n}}+O(q)\right)\frac{d}{dt}e(\beta t)\,dt+ \\ +\left(\frac{S(q,a)}{q}P+O(q)\right)e\left(\beta N\right)$$

След това разкриваме скобите и използвайки Лема 27, както и оценката

$$\frac{d}{dt}e(\beta t)=2\pi i\beta e(\beta t)\ll|\beta|,$$

намираме, че

$$V\left(\frac{a}{q}+\beta\right)=\frac{S(q,a)}{q}\left(-\int\limits_0^N t^{\frac{1}{n}}\frac{d}{dt}e(\beta t)\,dt+Pe(\beta N)\right)+O(q(1+N|\beta|)). \tag{215}$$

Като интегрираме по части и вземем предвид (156), получаваме, че главният член в (215) е равен на

$$\frac{S(q,a)}{q}\int\limits_0^N e(\beta t)\,\frac{1}{n}\,t^{\frac{1}{n}-1}\,dt.$$

Заместваме в (215) и намираме

$$V\left(\frac{a}{q}+\beta\right)=\frac{S(q,a)}{q}\int\limits_0^N e(\beta t)\,\frac{1}{n}\,t^{\frac{1}{n}-1}\,dt+O(q(1+N|\beta|)). \tag{216}$$

Ще покажем, че интегралът в (216) може да се замени с израза $W(\beta)$, определен чрез (210), като получената грешка не надхвърля порядъка на остатъчния член в

(209). За целта прилагаме към $W(\beta)$ сумационната формула на Ойлер (Лема 32) и получаваме

$$W(\beta) = \frac{1}{n}\int\limits_{1/2}^{N} e(\beta t)\, t^{\frac{1}{n}-1}\, dt + O(1) - \frac{1}{n}\int\limits_{1/2}^{N} \rho(t)\frac{d}{dt}\left(e(\beta t)\, t^{\frac{1}{n}-1}\right)\, dt.$$

Променяме долната граница на първия интеграл от 1/2 на 0 с грешка от порядък $O(1)$. Използваме също определението на $\rho(t)$, дадено в Лема 32 и намираме, че

$$\begin{aligned} W(\beta) - \frac{1}{n}\int\limits_{0}^{N} e(\beta t)\, t^{\frac{1}{n}-1}\, dt \; &\ll \; 1 + \int\limits_{1/2}^{N} \left|\frac{d}{dt}\left(e(\beta t)\, t^{\frac{1}{n}-1}\right)\right| dt \\ &\ll 1 + \int\limits_{1/2}^{N} t^{\frac{1}{n}-1}|\beta|\, dt + \int\limits_{1/2}^{N} t^{\frac{1}{n}-2}\, dt \\ &\ll 1 + |\beta| N. \end{aligned}$$

От горната оценка и от (216) следва (209), с което лемата е доказана. □

Да продължим изследването на I'. Нека означим

$$A = V\left(\frac{a}{q} + \beta\right), \qquad B = \frac{S(q,a)}{q} W(\beta). \tag{217}$$

Използваме (156), (159) и Лема 17 и виждаме, че ако са налице условията (208), то

$$A - B \ll q(1 + |\beta| N) \ll q + \frac{N}{\tau} \ll Q. \tag{218}$$

От (158), (210), (217) и Лема 32 следва

$$A \ll P, \qquad B \ll |W(\beta)| \ll N^{1/n} = P. \tag{219}$$

Тогава имаме

$$A^k - B^k = (A - B)\left(A^{k-1} + A^{k-2}B + \ldots + AB^{k-2} + B^{k-1}\right) \ll Q\, P^{k-1}. \tag{220}$$

Като използваме (217), (218) и (220) виждаме, че подинтегралната функция в (207) е равна на

$$\left(\frac{S(q,a)}{q}\right)^k e\left(-\frac{aN}{q}\right)\, W^k(\beta)\, e(-N\beta) + O\left(Q\, P^{k-1}\right).$$

Оттук и от (207) следва

$$I' = \sum_{q \le Q} \gamma(q) \int\limits_{-1/(q\tau)}^{1/(q\tau)} W^k(\beta)\, e(-N\beta)\, d\beta + O\left(\Delta^*\right), \tag{221}$$

където

$$\gamma(q) = \gamma_{k,n,N}(q) = \sum_{\substack{a=0 \\ (a,q)=1}}^{q-1} \left(\frac{S(q,a)}{q} \right)^k e\left(-\frac{aN}{q} \right), \tag{222}$$

$$\Delta^* = \sum_{q \le Q} \sum_{a=0}^{q-1} \frac{QP^{k-1}}{q\tau} \ll Q^2 P^{k-1} \tau^{-1}. \tag{223}$$

Като използваме (156) и (159) виждаме, че

$$\Delta^* \ll N^{\frac{k}{n}-1-\delta}, \qquad \delta = \delta(k,n) > 0. \tag{224}$$

Да разгледаме интеграла в (221). Ще го заменим с интеграл по интервала $\left[-\frac{1}{2}, \frac{1}{2}\right]$ и, за да оценим грешката при тази замяна, ще докажем следната

Лема 18. *За израза* $W(\beta)$*, определен чрез* (210)*, е в сила*

$$W(\beta) \ll \min\left(P\,,\, \|\beta\|^{-\frac{1}{n}} \right). \tag{225}$$

Доказателство. От втората оценка, дадена в (219) виждаме, че е достатъчно да докажем неравенството

$$W(\beta) \ll \|\beta\|^{-\frac{1}{n}} \qquad \text{при} \qquad \beta \notin \mathbb{Z}. \tag{226}$$

От (210) и Лема 27 следва, че функцията $W(\beta)$ е четна и освен това периодична с период 1. Очевидно, функцията $\|\beta\|$ притежава същото свойство. Следователно е достатъчно да докажем, че

$$W(\beta) \ll \beta^{-\frac{1}{n}} \tag{227}$$

при $0 < \beta \le \frac{1}{2}$. Ако $P \le \beta^{-\frac{1}{n}}$, то (227) е следствие от (219).

Нека $P > \beta^{-\frac{1}{n}}$, или, все едно

$$\frac{1}{N} < \beta \le \frac{1}{2}. \tag{228}$$

Тогава можем да запишем $W(\beta)$ във вида

$$W(\beta) = W_1 + W_2, \tag{229}$$

където

$$W_1 = \frac{1}{n} \sum_{1 \le m \le \frac{1}{\beta}} e(\beta m)\, m^{\frac{1}{n}-1}, \qquad W_2 = \frac{1}{n} \sum_{\frac{1}{\beta} < m \le N} e(\beta m)\, m^{\frac{1}{n}-1}. \tag{230}$$

Използвайки Лема 32, получаваме

$$W_1 \ll \sum_{m \le \frac{1}{\beta}} m^{\frac{1}{n}-1} \ll \beta^{-\frac{1}{n}}. \tag{231}$$

За W_2 прилагаме преобразуванието на Абел (Лема 31) и намираме, че

$$W_2 = -\frac{1}{n} \int\limits_{\frac{1}{\beta}}^{N} \left(\sum_{\frac{1}{\beta} < m \le t} e(\beta m) \right) \frac{d}{dt} \left(t^{\frac{1}{n}-1} \right) dt + \frac{1}{n} \sum_{\frac{1}{\beta} < m \le N} e(\beta m) \, N^{\frac{1}{n}-1}$$

От горното равенство, Лема 5 и условието (228) получаваме

$$|W_2| \ll \int\limits_{\frac{1}{\beta}}^{N} \left| \sum_{\frac{1}{\beta} < m \le t} e(\beta m) \right| t^{\frac{1}{n}-2} \, dt + \left| \sum_{\frac{1}{\beta} < m \le N} e(\beta m) \right| N^{\frac{1}{n}-1}$$

$$\ll \frac{1}{\beta} \left(\int\limits_{\frac{1}{\beta}}^{N} t^{\frac{1}{n}-2} \, dt + N^{\frac{1}{n}-1} \right) \ll \frac{1}{\beta} \left(\frac{1}{\beta} \right)^{\frac{1}{n}-1}$$

$$\ll \beta^{-\frac{1}{n}}. \tag{232}$$

От (229), (231) и (232) следва (227). С това лемата е доказана. □

Да се върнем към изследването на I'. Означаваме

$$R(N) = R_{k,n}(N) = \int\limits_{-1/2}^{1/2} W^k(\beta) \, e(-N\beta) \, d\beta. \tag{233}$$

Тогава имаме

$$\int\limits_{-1/(q\tau)}^{1/(q\tau)} W^k(\beta) \, e(-N\beta) \, d\beta = R(N) + O\left(\Delta^{**}\right), \tag{234}$$

където

$$\Delta^{**} = \int\limits_{\frac{1}{q\tau} \le |\beta| \le \frac{1}{2}} |W(\beta)|^k \, d\beta. \tag{235}$$

Ясно е, че от Лема 18 следва

$$\Delta^{**} \ll \int\limits_{1/(q\tau)}^{\infty} \frac{d\beta}{\beta^{\frac{k}{n}}} \ll (q\tau)^{\frac{k}{n}-1}. \tag{236}$$

Като вземем предвид (221), (224), (234) и (236) виждаме, че

$$I' = \sum_{q \le Q} \gamma(q) \left(R(N) + O\left((q\tau)^{\frac{k}{n}-1} \right) \right) + O\left(N^{\frac{k}{n}-1-\delta} \right)$$

$$= R(N) \sum_{q \le Q} \gamma(q) + O\left(\sum_{q \le Q} |\gamma(q)| (q\tau)^{\frac{k}{n}-1} \right) + O\left(N^{\frac{k}{n}-1-\delta} \right), \qquad \delta = \delta(k,n) > 0. \tag{237}$$

За да оценим първия от горните два остатъчни члена ще докажем следната

Лема 19. *Нека* $n \ge 2$ *и* $k \ge 2^n + 1$. *Тогава е изпълнено*

$$\gamma(q) \ll q^{-1-\frac{1}{2^n}}. \tag{238}$$

Доказателство. Ще използваме теоремата на Херман Вайл (Лема 15). Прилагаме я за $P = q$ и $f(x) = ax^n/q$ и получаваме

$$S(q,a) = \sum_{x=1}^{q} e\left(\frac{ax^n}{q} \right) \ll q^{1+\varepsilon} \left(\frac{1}{q} + \frac{1}{q} + \frac{q}{q^n} \right)^{\frac{1}{2^{n-1}}} \ll q^{1+\varepsilon-\frac{1}{2^{n-1}}}.$$

Тогава от (222) следва

$$|\gamma(q)| \le \sum_{\substack{a=0 \\ (a,q)=1}}^{q-1} \left| \frac{S(q,a)}{q} \right|^k \ll q^{1+\left(\varepsilon - \frac{1}{2^{n-1}}\right)k}.$$

Като използваме условието $k \ge 2^n + 1$ и предефинираме ε получаваме

$$\gamma(q) \ll q^{1-\frac{k}{2^{n-1}}+\varepsilon} \ll q^{1-\frac{2^n+1}{2^{n-1}}+\varepsilon} \ll q^{1-2-\frac{1}{2^n}} = q^{-1-\frac{1}{2^n}}. \tag{239}$$

С това лемата е доказана. □

От тази лема, от (156) и (159) следва, че първият остатъчен член в (237) е

$$\ll \tau^{\frac{k}{n}-1} \sum_{q \le Q} q^{\frac{k}{n}-\frac{1}{2^n}-2} \ll \tau^{\frac{k}{n}-1} Q^{\frac{k}{n}-\frac{1}{2^n}-1} \ll N^{\frac{k}{n}-1-\frac{1}{100 \cdot n 2^n}}$$

и, като използваме (237), получаваме

$$I' = R(N) \sum_{q \le Q} \gamma(q) + O\left(N^{\frac{k}{n}-1-\delta} \right), \qquad \delta = \delta(k,n) > 0. \tag{240}$$

Сега ще изследваме величината $R(N)$. От (210) и (233) получаваме

$$R(N) = \int_{-1/2}^{1/2} \left(\frac{1}{n} \sum_{m=1}^{N} m^{\frac{1}{n}-1} e(\beta m) \right)^k e(-\beta N)\, d\beta$$

$$= \frac{1}{n^k} \sum_{1 \le m_1, \dots, m_k \le N} (m_1 \dots m_k)^{\frac{1}{n}-1} \int_{-1/2}^{1/2} e\left((m_1 + \dots + m_k - N)\beta \right)\, d\beta.$$

Сега, като приложим Лема 27, намираме

$$R(N) = \frac{1}{n^k} \sum_{m_1+\dots+m_k=N} (m_1 \dots m_k)^{\frac{1}{n}-1} . \tag{241}$$

Предстои ни да намерим асимптотична формула за тази величина. За целта първо ще докажем следната

Лема 20. *Нека $\alpha, \beta \in \mathbb{R}$, $0 < \alpha < 1$, $\alpha \le \beta$. Тогава за всяко $M \in \mathbb{N}$ е в сила формулата*

$$\sum_{1 \le m \le M-1} m^{\alpha-1}(M-m)^{\beta-1} = \frac{\Gamma(\alpha)\Gamma(\beta)}{\Gamma(\alpha+\beta)} M^{\alpha+\beta-1} + O\left(M^{\beta-1}\right),$$

където $\Gamma(t)$ е Гама-функцията на Ойлер, а константата в знака O зависи само от α и β.

Доказателство. Можем да считаме, че $M \ge 3$, тъй като в противен случай твърдението е тривиално. Разглеждаме функцията

$$f(t) = t^{\alpha-1}(M-t)^{\beta-1}$$

при $1 \le t \le M-1$. Лесно се вижда, че

$$f(t) = O\left(M^{\beta-1}\right) \qquad \text{равномерно при} \qquad t \in [1, M-1]. \tag{242}$$

Тогава, като използваме сумационната формула на Ойлер (Лема 32), получаваме

$$\sum_{m=1}^{M-1} f(m) = \int_1^{M-1} f(t)\, dt + O\left(M^{\beta-1}\right) + O\left(\int_1^{M-1} |f'(t)|\, dt\right). \tag{243}$$

Не е трудно да се установи, че функцията $f'(t)$ може да се анулира в не повече от една точка от интервала $(1, M-1)$. Ако такава е точката ξ, то $f'(t)$ не се анулира в интервалите $(1, \xi)$ и $(\xi, M-1)$. От този факт, от теоремата на Лайбниц и Нютон и от (242) следва

$$\begin{aligned}
\int_1^{M-1} |f'(t)|\, dt &= \int_1^{\xi} |f'(t)|\, dt + \int_{\xi}^{M-1} |f'(t)|\, dt \\
&= \left| \int_1^{\xi} f'(t)\, dt \right| + \left| \int_{\xi}^{M-1} f'(t)\, dt \right| \\
&= |f(\xi) - f(1)| + |f(M-1) - f(\xi)| \\
&\ll M^{\beta-1}.
\end{aligned}$$

Ясно е, че същата оценка е изпълнена и в случая когато $f'(t)$ не се анулира в интервала $(1, M-1)$.

По-нататък, непосредствено се проверява, че интегралите $\int_0^1 f(t)dt$ и $\int_{M-1}^M f(t)dt$ са сходящи и се оценяват като $O\left(M^{\beta-1}\right)$. Сега от (243) и от горните разсъждения следва

$$\sum_{m=1}^{M-1} f(m) = \int\limits_0^M f(t)\,dt + O\left(M^{\beta-1}\right).$$

Остава да забележим, че след смяна на променливата и прилагане на Лема 34 получаваме

$$\int\limits_0^M f(t)\,dt = M^{\alpha+\beta-1}\int\limits_0^1 t^{\alpha-1}(1-t)^{\beta-1}\,dt = \frac{\Gamma(\alpha)\Gamma(\beta)}{\Gamma(\alpha+\beta)}M^{\alpha+\beta-1}.$$

С това лемата е доказана. □

Следващата стъпка е доказателството на следната

Лема 21. *Нека $n, k \in \mathbb{N}$, $n \geq 2$, $k \geq 2$. При $M \in \mathbb{N}$ за величината*

$$R_{k,n}(M) = \frac{1}{n^k}\sum_{m_1+\cdots+m_k=M}(m_1\ldots m_k)^{\frac{1}{n}-1}$$

е в сила формулата

$$R_{k,n}(M) = \frac{\Gamma\left(1+\frac{1}{n}\right)^k}{\Gamma\left(\frac{k}{n}\right)}M^{\frac{k}{n}-1} + O\left(M^{\frac{k-1}{n}-1}\right),$$

където $\Gamma(t)$ е Гама-функцията на Ойлер, а константата в знака O зависи само от k и n.

Доказателство. Ще работим чрез индукция по k. При $k=2$ твърдението следва непосредствено от Лема 20.

Да допуснем, че твърдението е доказано при някое $k \geq 2$ за всички $M \in \mathbb{N}$ и да разгледаме $R_{k+1,n}(M)$. Да отбележим, че ако $M \leq c(k,n)$, то формулата която искаме да докажем очевидно е вярна. Тогава можем да считаме, че M е достатъчно голямо спрямо k и n. Имаме

$$\begin{aligned} R_{k+1,n}(M) &= \frac{1}{n^{k+1}}\sum_{m_1+\cdots+m_{k+1}=M}(m_1\ldots m_{k+1})^{\frac{1}{n}-1} \\ &= \frac{1}{n}\sum_{1\leq m\leq M-k} m^{\frac{1}{n}-1}\,\frac{1}{n^k}\sum_{m_1+\cdots+m_k=M-m}(m_1\ldots m_k)^{\frac{1}{n}-1} \\ &= \frac{1}{n}\sum_{1\leq m\leq M-k} m^{\frac{1}{n}-1}\,R_{k,n}(M-m). \end{aligned}$$

Използваме индукционното допускане и, като извършим някои очевидни пресмятания, получаваме

$$R_{k+1,n}(M) = \frac{1}{n} \sum_{1 \le m \le M-k} m^{\frac{1}{n}-1} \left(\frac{\Gamma\left(1+\frac{1}{n}\right)^k}{\Gamma(\frac{k}{n})} (M-m)^{\frac{k}{n}-1} + O\left(M^{\frac{k-1}{n}-1}\right) \right)$$

$$= \frac{\Gamma\left(1+\frac{1}{n}\right)^k}{n\,\Gamma(\frac{k}{n})} \sum_{1 \le m \le M-k} m^{\frac{1}{n}-1}(M-m)^{\frac{k}{n}-1} + O\left(M^{\frac{k}{n}-1}\right)$$

$$= \frac{\Gamma\left(1+\frac{1}{n}\right)^k}{n\,\Gamma(\frac{k}{n})} \sum_{1 \le m \le M-1} m^{\frac{1}{n}-1}(M-m)^{\frac{k}{n}-1} + O\left(M^{\frac{k}{n}-1}\right).$$

Заместваме последната сума по m със съответния израз, даден в Лема 20, след което прилагаме Лема 34 и намираме

$$R_{k+1,n}(M) = \frac{\Gamma\left(1+\frac{1}{n}\right)^k}{n\,\Gamma(\frac{k}{n})} \, \frac{\Gamma\left(\frac{1}{n}\right)\Gamma\left(\frac{k}{n}\right)}{\Gamma(\frac{k+1}{n})} M^{\frac{k+1}{n}-1} + O\left(M^{\frac{k}{n}-1}\right)$$

$$= \frac{\Gamma\left(1+\frac{1}{n}\right)^{k+1}}{\Gamma(\frac{k+1}{n})} M^{\frac{k+1}{n}-1} + O\left(M^{\frac{k}{n}-1}\right).$$

С това лемата е доказана. □

От тази лема следва, че за величината $R(N)$, определена чрез (241), имаме

$$R(N) = \frac{\Gamma\left(1+\frac{1}{n}\right)^k}{\Gamma(\frac{k}{n})} N^{\frac{k}{n}-1} + O\left(N^{\frac{k-1}{n}-1}\right). \tag{244}$$

По-нататък, от (239) следва $\sum_{q \le Q} \gamma(q) \ll 1$. Поради това от (240) и (244) получаваме

$$I' = \frac{\Gamma\left(1+\frac{1}{n}\right)^k}{\Gamma(\frac{k}{n})} N^{\frac{k}{n}-1} \sum_{q \le Q} \gamma(q) + O\left(N^{\frac{k}{n}-1-\delta}\right), \qquad \delta = \delta(k,n) > 0. \tag{245}$$

Следващата стъпка е да заменим крайната сума по q с безкрайния ред

$$\mathfrak{S}_{k,n}(N) = \sum_{q=1}^{\infty} \gamma(q) \tag{246}$$

и да оценим получената грешка. Да отбележим, че вследствие на оценката (239), редът (246) е абсолютно сходящ и за сумата му е изпълнено

$$|\mathfrak{S}_{k,n}(N)| \le c_2(k,n), \tag{247}$$

където $c_2(k,n)$ не зависи от N и $c_2(k,n) > 0$. Също така, от (156), (159) и (239) следва

$$\mathfrak{S}_{k,n}(N) - \sum_{q\le Q}\gamma(q) \ll \sum_{q>Q}|\gamma(q)| \ll \sum_{q>Q} q^{-1-\frac{1}{2^n}} \ll Q^{-\frac{1}{2^n}} \ll N^{-\frac{1}{100\cdot n2^n}}. \tag{248}$$

От (245) и (248) намираме

$$I' = \frac{\Gamma\left(1+\frac{1}{n}\right)^k}{\Gamma(\frac{k}{n})}\,\mathfrak{S}_{k,n}(N)\,N^{\frac{k}{n}-1} + O\left(N^{\frac{k}{n}-1-\delta}\right), \qquad \delta=\delta(k,n)>0. \tag{249}$$

3.2.4 Изследване на особения ред $\mathfrak{S}_{k,n}(N)$.

От (162), (206) и (249) намираме

$$I_{k,n}(N) = \frac{\Gamma\left(1+\frac{1}{n}\right)^k}{\Gamma(\frac{k}{n})}\,\mathfrak{S}_{k,n}(N)\,N^{\frac{k}{n}-1} + O\left(N^{\frac{k}{n}-1-\delta}\right), \qquad \delta=\delta(k,n)>0. \tag{250}$$

С това формулата (154) от условието на теоремата е доказана. Остава да изучим величината $\mathfrak{S}_{k,n}(N)$, определена чрез (246), и да установим неравенствата (155) Първо ще докажем следната

Лема 22. *Функцията $\gamma(q)$, определена чрез* (222), *е мултипликативна по отношение на q.*

Доказателство: Очевидно $\gamma(1) = 1$. По-нататък, нека $q_1, q_2 \in \mathbb{N}$, $(q_1, q_2) = 1$. Според Лема 46 имаме

$$\gamma(q_1q_1) = \sum_{\substack{a=0\\(a,q_1q_2)=1}}^{q_1q_2-1}\left(\frac{S(q_1q_2,a)}{q_1q_2}\right)^k e\left(-\frac{aN}{q_1q_2}\right)$$

$$= \sum_{\substack{a_1=0\\(a_1,q_1)=1}}^{q_1-1}\ \sum_{\substack{a_2=0\\(a_2,q_2)=1}}^{q_2-1}\left(\frac{S(q_1q_2,a_1q_2+a_2q_1)}{q_1q_2}\right)^k e\left(-\frac{(a_1q_2+a_2q_1)N}{q_1q_2}\right). \tag{251}$$

Като използваме (211) и Лема 46 получаваме

$$S(q_1q_2, a_1q_2+a_2q_1) = \sum_{x=1}^{q_1q_2} e\left(\frac{(a_1q_2+a_2q_1)x^n}{q_1q_2}\right)$$

$$= \sum_{x_1=1}^{q_1}\ \sum_{x_2=1}^{q_2} e\left(\frac{(a_1q_2+a_2q_1)(x_1q_2+x_2q_1)^n}{q_1q_2}\right).$$

Оттук, от Лема 27 и от Лема 46 следва

$$S(q_1q_2, a_1q_2 + a_2q_1) = \sum_{x_1=1}^{q_1} \sum_{x_2=1}^{q_2} e\left(\frac{(a_1q_2 + a_2q_1)(x_1^n q_2^n + x_2^n q_1^n)}{q_1q_2}\right)$$

$$= \sum_{x_1=1}^{q_1} \sum_{x_2=1}^{q_2} e\left(\frac{a_1 x_1^n q_2^{n+1} + a_2 x_2^n q_1^{n+1}}{q_1q_2}\right)$$

$$= \sum_{x_1=1}^{q_1} e\left(\frac{a_1(x_1q_2)^n}{q_1}\right) \sum_{x_2=1}^{q_2} e\left(\frac{a_2(x_2q_1)^n}{q_2}\right)$$

$$= S(q_1, a_1)S(q_2, a_2).$$

Като заместим в (251) и използваме (222) получаваме

$$\gamma(q_1q_2) = \gamma(q_1)\gamma(q_2).$$

С това лемата е доказана. □

От абсолютната сходимост на реда, представящ $\mathfrak{S}_{k,n}(N)$, и от Лема 22 виждаме, че можем да приложим тъждеството на Ойлер (Лема 35). Получаваме

$$\mathfrak{S}_{k,n}(N) = \prod_p T(p), \tag{252}$$

където

$$T(p) = T_{k,n,N}(p) = \sum_{l=0}^{\infty} \gamma\left(p^l\right). \tag{253}$$

За да получим информация за $T(p)$ ще се възползваме от следната

Лема 23. *Нека $M(q) = M_{k,n,N}(q)$ е броят на решенията на сравнението*

$$x_1^n + \cdots + x_k^n \equiv N \pmod q.$$

Тогава е в сила формулата

$$\sum_{d|q} \gamma(d) = \frac{M(q)}{q^{k-1}}.$$

Доказателство. Като използваме Лема 27, записваме $M(q)$ във вида

$$M(q) = \sum_{1\le x_1,\ldots,x_k\le q} \frac{1}{q} \sum_{k=1}^{q} e\left(\frac{k\left(x_1^n + \cdots + x_k^n - N\right)}{q}\right).$$

Разделяме сумата по k на части съобразно стойността на (k,q), след което отново използваме Лема 27. Получаваме

$$M(q)=\frac{1}{q}\sum_{d|q}\sum_{\substack{k=1\\(k,q)=\frac{q}{d}}}^{q}\sum_{1\le x_1,\ldots,x_k\le q}e\left(\frac{k\left(x_1^n+\cdots+x_k^n-N\right)}{q}\right)$$

$$=\frac{1}{q}\sum_{d|q}\sum_{\substack{a=1\\(a,d)=1}}^{d}\sum_{1\le x_1,\ldots,x_k\le q}e\left(\frac{a\left(x_1^n+\cdots+x_k^n-N\right)}{d}\right)$$

$$=\frac{1}{q}\sum_{d|q}\sum_{\substack{a=1\\(a,d)=1}}^{d}e\left(-\frac{aN}{d}\right)\left(\sum_{x=1}^{q}e\left(\frac{ax^n}{d}\right)\right)^k.$$

Очевидно при $d\mid q$ имаме

$$\sum_{x=1}^{q}e\left(\frac{ax^n}{d}\right)=\frac{q}{d}\,S(d,a),$$

където $S(d,a)$ се определя от (211). Тогава от горните формули и от (222) намираме

$$M(q)=q^{k-1}\sum_{d|q}\sum_{\substack{a=1\\(a,d)=1}}^{d}\left(\frac{S(d,a)}{d}\right)^k e\left(-\frac{aN}{d}\right)=q^{k-1}\sum_{d|q}\gamma(d),$$

с което лемата е доказана. □

Нека приложим тази лема при $q=p^r$, където p е просто число. Получаваме

$$\sum_{l=0}^{r}\gamma\left(p^l\right)=\frac{M\left(p^r\right)}{p^{r(k-1)}}.$$

Извършваме граничен преход $r\to\infty$ и, като вземем предвид (253), получаваме

$$T(p)=\lim_{r\to\infty}\frac{M\left(p^r\right)}{p^{r(k-1)}}. \tag{254}$$

Тъй като е очевидно, че $M(q)\ge 0$, то от (254) следва

$$T(p)\ge 0 \qquad \text{за всяко } p. \tag{255}$$

Но тогава от (252) и (255) получаваме $\mathfrak{S}_{k,n}(N)\ge 0$. Последното неравенство, заедно с (247), ни дава

$$0\le\mathfrak{S}_{k,n}\le c_2(k,n), \tag{256}$$

където $c_2(k,n)$ не зависи от N и $c_2(k,n)>0$.

Оценката отдолу за $\mathfrak{S}_{k,n}(N)$ от формула (256) не е достатъчно добра, за да сме сигурни, че главният член в асимптотичната формула (154) доминира над остатъчния член. За да установим, че в сила оценката отдолу от (155), са необходими допълнителни изследвания.

От (253) следва

$$T(p) \geq 1 - \Delta^{\#}, \qquad \Delta^{\#} = \sum_{l=1}^{\infty} \left|\gamma\left(p^l\right)\right|. \tag{257}$$

Като използваме (238), получаваме

$$\Delta^{\#} \ll \sum_{l=1}^{\infty} p^{-l\left(1+\frac{1}{2^n}\right)} \ll p^{-1-\frac{1}{2^n}}.$$

Следователно съществува $c^* = c^*(k,n) > 0$, такова че

$$|\Delta^{\#}| \leq p^{-1-\frac{1}{2^{n-1}}} \qquad \text{при} \qquad p > c^*. \tag{258}$$

Оттук получаваме

$$\prod_{p>c^*} T(p) \geq c^{**}(k,n), \qquad c^{**}(k,n) = \prod_{p>c^*} \left(1 - p^{-1-\frac{1}{2^{n-1}}}\right) > 0. \tag{259}$$

От формулите (252), (255) и (259) намираме

$$\mathfrak{S}_{k,n}(N) \geq c^{**}(k,n) \prod_{p \leq c^*(k,n)} T(p). \tag{260}$$

Остава да намерим нетривиална оценка отдолу за $T(p)$ при $p \leq c^*$. За тази цел са ни необходими още три леми.

Да представим числото n във вида

$$n = p^{\tau} n_1, \qquad p \nmid n_1. \tag{261}$$

Определяме

$$\gamma = \begin{cases} \tau + 1 & \text{при} \qquad p > 2, \\ \tau + 2 & \text{при} \qquad p = 2. \end{cases} \tag{262}$$

Лема 24. *Нека $k, n \in \mathbb{N}$, $n \geq 2$ и $k \geq k_0(n)$, където*

$$k_0(n) = \begin{cases} 5 & \textit{при} \qquad n = 2, \\ 2n & \textit{при} \qquad 2 \nmid n, \\ 4n & \textit{при} \qquad 2 \mid n, \quad n > 2. \end{cases} \tag{263}$$

Нека p е просто число и γ е определено чрез (262). Тогава за всяко $N \in \mathbb{Z}$ сравнението

$$x_1^n + \cdots + x_k^n \equiv N \pmod{p^{\gamma}}. \tag{264}$$

притежава решение в цели числа $x_1, \ldots, x_k$, поне едно от които не се дели на p.

Доказателство. Достатъчно е да установим, че ако

$$k \geq k_0(n) - 1, \tag{265}$$

то за всяко $N \in \mathbb{Z}$, за което $p \nmid N$, сравнението (264) е разрешимо в цели числа $x_1, \dots .x_k$.

Наистина, да допуснем, че сме доказали това твърдение. Нека вземем произволно $N \in \mathbb{Z}$ и нека $k \geq k_0(n)$. Ако $p \nmid N$, то, според нашето допускане, (264) ще е разрешимо и очевидно поне едно x_j няма да се дели на p. Ако пък е изпълнено $p \mid N$, то $p \nmid N - 1$. Тъй като $k - 1 \geq k_0(n) - 1$, то като използваме отново нашето допускане, виждаме, че съществуват $y_1, \dots, y_{k-1} \in \mathbb{Z}$, за които

$$y_1^n + \cdots + y_{k-1}^n \equiv N - 1 \pmod{p^\gamma},$$

откъдето

$$y_1^n + \cdots + y_{k-1}^n + 1^n \equiv N \pmod{p^\gamma}.$$

Или отново виждаме, че (264) е разрешимо, като поне едно x_j не се дели на p.

И тъй, оттук нататък считаме, че $p \nmid N$ и че е изпълнено условието (265), като нашата цел е да докажем разрешимостта на (264) е цели числа $x_1, \dots, x_k$.

Ще разгледаме първо случая $p > 2$. Очевидно можем да считаме, че N принадлежи на множеството

$$\mathcal{N} = \{ \, N \in \mathbb{N} \, : \, 1 \leq N \leq p^\gamma, \; p \nmid N \, \}.$$

За всяко $N \in \mathcal{N}$ означаваме с $\kappa(N)$ най-малкото естествено число k, за което (264) е разрешимо относно $x_1, \dots, x_k$. Да отбележим, че всяко $N \in \mathcal{N}$ е сума на N на брой n-ти степени на 1, следователно определението на $\kappa(N)$ е коректно.

В множеството $\mathcal{N}$ определяме релацията „$\sim$" по следния начин. Ако $N_1, N_2 \in \mathcal{N}$ считаме, че $N_1 \sim N_2$ когато $\kappa(N_1) = \kappa(N_2)$. Очевидно „$\sim$" е релация на еквивалентност. Ще проверим, че са налице следните свойства:

1) Ако $N_1, N_2 \in \mathcal{N}$ и

$$N_1 \equiv N_2 \, z^n \pmod{p^\gamma} \qquad \text{за някое} \qquad z \in \mathbb{Z}, \tag{266}$$

то $N_1 \sim N_2$.

2) Множеството $\mathcal{N}$ се разбива на не повече от n на брой класа на еквивалентност относно „$\sim$".

Да докажем първо 1). Нека $N_1, N_2 \in \mathcal{N}$ и нека е изпълнено (266). Полагаме $k_j = \kappa(N_j)$, $j = 1, 2$. От определението на k_2 следва, че

$$x_1^n + \cdots + x_{k_2}^n \equiv N_2 \pmod{p^\gamma}$$

за някакви $x_1, \dots, x_{k_2} \in \mathbb{Z}$. От това сравнение и от (266) следва

$$(x_1 z)^n + \cdots + (x_{k_2} z)^n \equiv N_2\, z^n \equiv N_1 \pmod{p^\gamma}.$$

Но тогава, като използваме определението на k_1, получаваме $k_1 \le k_2$.

От друга страна, числото z от (266) не се дели на p, следователно, според Лема 48, можем да намерим $\overline{z} \in \mathbb{Z}$, такова че $z\,\overline{z} \equiv 1 \pmod{p^\gamma}$. Но тогава от (266) следва $N_2\,\overline{z}^n \equiv N_1 \pmod{p^\gamma}$ и, като повторим предишните разсъждения, получаваме $k_2 \le k_1$. И така, установихме, че $k_1 = k_2$, което означава, че $N_1 \sim N_2$.

Сега ще докажем свойство 2). Нека $\mathcal{N}$ се разбива на m класа на еквивалентност относно $\sim$ с представители съответно $N_1, \dots, N_m$. Тъй като разглеждаме случая $p > 2$, то според Лема 50 съществува примитивен корен g по модул p^γ. Тогава за някои $\alpha_1, \dots, \alpha_m \in \mathbb{N}$ е изпълнено $N_j \equiv g^{\alpha_j} \pmod{p^\gamma}$ при $j = 1, \dots, m$. Числата α_j са две по две несравними по модул n. Наистина, ако допуснем, например, че $\alpha_1 \equiv \alpha_2 \pmod{n}$, то $\alpha_1 = \alpha_2 + hn$ за някое $h \in \mathbb{Z}$. Без ограничение на общността можем да считаме, че $h \ge 0$. Тогава ще имаме

$$N_1 \equiv g^{\alpha_1} = g^{\alpha_2 + hn} \equiv N_2 \left(g^h\right)^n \pmod{p^\gamma}$$

и от свойство 1) ще следва, че $N_1 \sim N_2$. Но това е невъзможно, тъй като N_1 и N_2 са представители на различни класове.

И така, числата $\alpha_1, \dots, \alpha_m$ принадлежат на различни класове от остатъци по модул n, а това е възможно само ако $m \le n$. С това свойство 2) е доказано.

Да продължим с доказателството на лемата в случая $p > 2$. От всеки клас на еквивалентност избираме най-малкия елемент и подреждаме получените числа по големина. Нека сме получили редицата

$$N_1 < N_2 < \cdots < N_m. \tag{267}$$

Ще проверим, че

$$\kappa(N_j) \le 2j - 1 \qquad \text{при} \qquad 1 \le j \le m. \tag{268}$$

За да докажем това твърдение ще използваме индукция по j. Очевидно $N_1 = 1$, следователно

$$\kappa(N_1) = \kappa(1) = 1 = 2 \cdot 1 - 1,$$

следователно твърдението е вярно при $j = 1$.

Нека $1 < j \le m$ и да допуснем, че $\kappa(N_\nu) \le 2\nu - 1$ при $1 \le \nu \le j - 1$. За да оценим отгоре $\kappa(N_j)$, разглеждаме числото $N_j - 1$.

Ако $p \nmid N_j - 1$, то като вземем предвид, че $N_j > N_1 = 1$, получаваме, че $N_j - 1 \in \mathcal{N}$. Следователно $N_j - 1$ се съдържа в някой от класовете на еквивалентност, т.е. $N_j - 1 \sim$

N_ν за някое $\nu \le m$. Оттук и от избора на числата (267) получаваме $N_\nu \le N_j - 1$, а това е възможно само ако $\nu \le j-1$. Сега от индукционното предположение следва

$$\kappa(N_j - 1) = \kappa(N_\nu) \le 2\nu - 1 \le 2(j-1) - 1 = 2j - 3.$$

Тогава за някое естествено число $s \le 2j-3$ съществуват $x_1, \dots, x_s \in \mathbb{Z}$ такива, че

$$x_1^n + \cdots + x_s^n \equiv N_j - 1 \pmod{p^\gamma},$$

или, все едно,

$$1^n + x_1^n + \cdots + x_s^n \equiv N_j \pmod{p^\gamma}.$$

Оттук следва $\kappa(N_j) \le s + 1 \le 2j - 2$.

Да разгледаме и случая $p \mid N_j - 1$. Тогава имаме $p \nmid N_j - 2$, откъдето следва, че $N_j - 2 \in \mathcal{N}$. Разсъждавайки както преди, намираме, че $N_j - 2 \sim N_\nu$ за някое $\nu \le j-1$. От индукционното предположение следва

$$\kappa(N_j - 2) = \kappa(N_\nu) \le 2\nu - 1 \le 2(j-1) - 1 = 2j - 3.$$

Тогава за някое естествено число $s \le 2j-3$ съществуват $x_1, \dots, x_s \in \mathbb{Z}$ такива, че

$$x_1^n + \cdots + x_s^n \equiv N_j - 2 \pmod{p^\gamma},$$

или, все едно,

$$1^n + 1^n + x_1^n + \cdots + x_s^n \equiv N_j \pmod{p^\gamma}.$$

Оттук следва $\kappa(N_j) \le s + 2 \le 2j - 1$. И така, индукционната стъпка е направена, с което неравенството (268) е доказано.

Нека $N \in \mathbb{N}$. Тогава $N \sim N_j$ за някое от числата (267). От (268) и от свойство 2) следва

$$\kappa(N) = \kappa(N_j) \le 2j - 1 \le 2m - 1 \le 2n - 1.$$

С това доказателството на лемата в случая $p > 2$ е завършено.

Остава да разгледаме случая $p = 2$. Ако $n = 2$, то от (261), (262) виждаме, че $\gamma = 3$ и твърдението е вярно, тъй като

$$1 \equiv 1^2, \quad 3 \equiv 1^2 + 1^2 + 1^2, \quad 5 \equiv 2^2 + 1^2, \quad 7 \equiv 2^2 + 1^2 + 1^2 + 1^2 \pmod 8.$$

Ако $2 \nmid n$ от (261), (262) следва $\gamma = 2$ и твърдението е вярно, тъй като

$$1 \equiv 1^n, \quad 3 \equiv 1^n + 1^n + 1^n \pmod 4.$$

Най-накрая ще разгледаме случая $2 \mid n$, $n > 2$. Тогава от (261), (262) получаваме $\tau \ge 1$ и $\gamma \ge 3$. При $N \in \mathcal{N}$ имаме

$$N \le 2^\gamma - 1 = 2^2 \cdot 2^\tau - 1 \le 4n - 1.$$

Тогава, ако $k \ge 4n - 1$, то е изпълнено $N = x_1^n + \cdots + x_k^n$, където $x_1 = \cdots = x_N = 1$ и $x_{N+1} = \cdots = x_k = 0$. С това твърдението е доказано и в този последен случай. Доказателството на лемата е завършено. □

Лема 25. *Дадени са $a \in \mathbb{Z}$, $y \in \mathbb{Z}$, $n \in \mathbb{N}$, $n \geq 2$ и просто число p. Нека γ е определено чрез* (262) *и нека е изпълнено*

$$y^n \equiv a \pmod{p^\gamma}, \qquad p \nmid y. \tag{269}$$

Тогава за всяко $r \in \mathbb{N}$, $r > \gamma$ сравнението

$$x^n \equiv a \pmod{p^r} \tag{270}$$

е разрешимо относно x.

Доказателство. Да разгледаме първо случая $p > 2$. От (269) следва $p \nmid a$. Според Лема 50 съществува примитивен корен g по модул p^r. Тогава от Лема 46 следва, че числата $g^b y^n$, където $b = 1, 2, \ldots, \varphi(p^r)$, образуват редуцирана система от остатъци по модул p^r. Следователно за някое $b \in \mathbb{N}$ имаме

$$g^b y^n \equiv a \pmod{p^r}. \tag{271}$$

От последното сравнение следва $g^b y^n \equiv a \pmod{p^\gamma}$. Като вземем предвид и (269), получаваме

$$g^b \equiv 1 \pmod{p^\gamma}. \tag{272}$$

Очевидно g е примитивен корен и по модул p^γ, следователно от (272) и от Лема 49 получаваме $b \equiv 0 \pmod{\varphi(p^\gamma)}$, или $b = \varphi(p^\gamma) b_1$ за някое $b_1 \in \mathbb{N}$. Тогава от Лема 42 и от (262) следва

$$b = p^{\gamma-1}(p-1)b_1 = p^\tau (p-1) b_1. \tag{273}$$

Да вземем произволно $h \in \mathbb{N}$. От горното равенство и Лема 42 получаваме

$$b + h\varphi(p^r) = p^\tau(p-1)b_1 + hp^{r-1}(p-1) = p^\tau(p-1)(b_1 + hp^{r-\tau-1}). \tag{274}$$

От условието (261) имаме $p \nmid n_1$. Тогава според Лема 48 съществува $h \in \mathbb{N}$ такова, че $n_1 \mid b_1 + hp^{r-\tau-1}$, т.е. $b_1 + hp^{r-\tau-1} = n_1 s$ за някое $s \in \mathbb{N}$. Ако h, s са избрани по описания по-горе начин, то от (261) и (274) намираме

$$b + h\varphi(p^r) = p^\tau(p-1)n_1 s = (p-1)ns. \tag{275}$$

Разглеждаме числото $x = y\, g^{(p-1)s}$. От (275) следва

$$x^n = y^n\, g^{(p-1)ns} = y^n\, g^b\, g^{h\varphi(p^r)}.$$

Тъй като $g^{\varphi(p^r)} \equiv 1 \pmod{p^r}$ и, като вземем предвид (271), виждаме, че x удовлетворява сравнението (270). С това твърдението в случая $p > 2$ е доказано.

Сега да разгледаме случая $p = 2$. Нека първо предположим, че $2 \nmid n$. Тогава, ако x пробягва редуцирана система от остатъци по модул 2^r, то такава система пробягва и x^n. Наистина, тези числа са $\varphi(2^r)$ на брой. Освен това те са две по две несравними по модул 2^r. За да установим този факт ще отбележим, че ако $2 \nmid x_1 x_2$, то $2 \nmid \left(x_1^{n-1} + x_1^{n-2} x_2 + \cdots + x_2^{n-1}\right)$. Тогава от тъждеството

$$x_1^n - x_2^n = (x_1 - x_2)\left(x_1^{n-1} + x_1^{n-2} x_2 + \cdots + x_2^{n-1}\right)$$

следва, че ако $x_1^n \equiv x_2^n \pmod{2^r}$, то $x_1 \equiv x_2 \pmod{2^r}$. Тогава за всяко $a \in \mathbb{Z}$, $2 \nmid a$ може да се намери x такова, че $x^n \equiv a \pmod{2^r}$.

Остана да разгледаме случая $p = 2$, $2 \mid n$. От (261) и (262) следва $\gamma \geq 3$. Да допуснем, че a, y удовлетворяват (269) (при $p = 2$). Според Лема 51 съществуват $\nu \in \mathbb{N}$, $b \in \mathbb{N}$ удовлетворяващи

$$1 \leq \nu \leq 2, \qquad 1 \leq b \leq 2^{r-2},$$

и такива, че

$$(-1)^\nu \, 5^b \, y^n \equiv a \pmod{2^r}.$$

Оттук следва, че $(-1)^\nu \, y^n \equiv a \pmod 4$ и понеже $y^n \equiv a \pmod 4$, то имаме $\nu = 2$. Следователно съществува $b \in \mathbb{N}$, такова че

$$5^b \, y^n \equiv a \pmod{2^\gamma}. \tag{276}$$

По-нататък разсъжденията са подобни на тези от случая $p > 2$. От (269) (при $p = 2$) и (276) следва, че $5^b \equiv 1 \pmod{2^\gamma}$ и според Лема 51 имаме $b \equiv 0 \pmod{2^{\gamma-2}}$. Следователно за някое $b_1 \in \mathbb{N}$ е изпълнено $b = 2^{\gamma-2} b_1 = 2^\tau b_1$. Ако $h \in \mathbb{N}$ разглеждаме числото $b + h 2^{r-2} = 2^\tau (b_1 + h 2^{r-\tau-2})$. От Лема 48 следва, че последното число се дели на n_1 при подходящо избрано h. Или можем да намерим $h \in \mathbb{N}$, $s \in \mathbb{N}$, така че $b_1 + h 2^{r-\tau-2} = n_1 s$ или, като вземем предвид (261), $b + h 2^{r-2} = ns$. Тогава, ако положим $x = y \, 5^s$, ще имаме $x^n = y^n \, 5^b \, 5^{h \, 2^{r-2}}$. От (276) и Лема 51 следва, че x удовлетворява (270) (при $p = 2$).

С това лемата е доказана. □

Лема 26. *Нека $k, n \in \mathbb{N}$, $n \geq 2$ и $k \geq k_0(n)$, където $k_0(n)$ е определено чрез* (263). *Нека p е просто число и γ е определено с* (262). *Тогава за всяко $N \in \mathbb{Z}$ и за всяко $r \in \mathbb{N}$, за което $r > \gamma$ сравнението*

$$x_1^n + \cdots + x_k^n \equiv N \pmod{p^r} \tag{277}$$

притежава поне $p^{(r-\gamma)(k-1)}$ решения.

Доказателство. Според Лема 24 сравнението

$$x_1^n + \cdots + x_k^n \equiv N \pmod{p^\gamma} \tag{278}$$

притежава решение $x_1, \ldots, x_k$, за което $p \nmid x_1$. Представяме (278) във вида

$$x_1^n \equiv N - x_2^n - \cdots - x_k^n \pmod{p^\gamma}.$$

Тогава за произволни $y_2, \ldots, y_k \in \mathbb{Z}$, за които

$$1 \leq y_2, \ldots, y_k \leq p^{r-\gamma}, \tag{279}$$

е изпълнено

$$x_1^n \equiv N - ((x_2 + p^\gamma y_2)^n + \cdots + (x_k + p^\gamma y_k)^n) \pmod{p^\gamma}.$$

Полагаме

$$z_i = x_i + p^\gamma y_i, \qquad 2 \le i \le k.$$

Според Лема 25 съществува z_1 такова, че $z_1^n \equiv N - z_2^n - \cdots - z_k^n \pmod{p^r}$, т.е.

$$z_1^n + \cdots + z_k^n \equiv N \pmod{p^r}.$$

Виждаме, че на всеки набор числа $y_2, \ldots, y_k$ удовлетворяващи (279) съответства решение на (277). Ако вземем друг набор $y'_2, \ldots, y'_k$, то ще получим друго решение $z'_1, \ldots, z'_k$. Наистина, ако имаме например $y_2 \neq y'_2$, то $p^\gamma y_2 \not\equiv p^\gamma y'_2 \pmod{p^r}$, откъдето $z_2 \not\equiv z'_2 \pmod{p^r}$.

Остава да отбележим, че броят на наборите $y_2, \ldots, y_k$, удовлетворяващи (279), е равен на $p^{(r-\gamma)(k-1)}$. С това лемата е доказана. $\square$

Сега вече можем да завършим доказателството на теоремата. От Лема 26 следва, че ако $k_0(n)$ е определено чрез (263), а γ – чрез (262), то за произволно просто p при $k \ge k_0(n)$ и $r > \gamma$ имаме

$$\frac{M(p^r)}{p^{r(k-1)}} \ge p^{-\gamma(k-1)}.$$

От последното неравенство и (254) получаваме

$$T(p) \ge p^{-\gamma(k-1)}.$$

Но тогава

$$\prod_{p \le c^*(k,n)} T(p) \ge c^\#(k,n), \qquad c^\#(k,n) = \prod_{p \le c^*(k,n)} p^{-\gamma(k-1)} > 0.$$

Като си припомним (256) и (260) получаваме

$$\mathfrak{S}_{k,n}(N) \ge c_1(k,n), \qquad c_1(k,n) = c^{**}(k,n)\, c^\#(k,n) > 0.$$

Тази оценка, заедно с (256), ни дава (155). С това Теорема 10 е доказана. $\square$

4 Допълнение

4.1 Функцията $e(\alpha)$.

В следната лема са събрани някои елементарни, но важни факти, отнасящи се до функцията $e(\alpha) = e^{2\pi i\alpha}$ при $\alpha \in \mathbb{R}$.

Лема 27. *При $\alpha \in \mathbb{R}$ функцията $e(\alpha)$ притежава следните свойства:*
(1) *$e(\alpha)$ е периодична с период 1.*
(2) *При $\alpha \in \mathbb{R}$ е изпълнено $|e(\alpha)| = 1$.*
(3) *При $\alpha \in \mathbb{Z}$ е изпълнено $e(\alpha) = 1$.*
(4) *За произволни $\alpha, \beta \in \mathbb{R}$ имаме $e(\alpha + \beta) = e(\alpha)e(\beta)$.*
(5) *Ако $n \in \mathbb{Z}$, то*

$$\int_0^1 e(\alpha n)d\alpha = \begin{cases} 1 & \text{при} \quad n = 0, \\ 0 & \text{при} \quad n \neq 0. \end{cases}$$

(6) *Ако $n \in \mathbb{Z}$, $q \in \mathbb{N}$, то*

$$\sum_{k=1}^{q} e\left(\frac{kn}{q}\right) = \begin{cases} q & \text{при} \quad n \equiv 0 \pmod q, \\ 0 & \text{в противен случай.} \end{cases}$$

Доказателство. Проверката на тези свойства е тривиална. □

4.2 Рационални приближения на реални числа.

Следното твърдение е известно като *лема на Дирихле* за приближаване на реални числа посредством рационални.

Лема 28. *Нека $\alpha, \tau \in \mathbb{R}, \tau \geq 1$. Съществуват $a \in \mathbb{Z}, q \in \mathbb{N}$, такива че*

$$\left|\alpha - \frac{a}{q}\right| < \frac{1}{q\tau}, \qquad (a, q) = 1, \qquad q \leq \tau.$$

Доказателство. Виж [1] гл. 1, зад. 4b. □

4.3 Някои известни неравенства

Твърдението в следващата лема е известно като *неравенство на триъгълника.*

Лема 29. *Ако $a_j \in \mathbb{C}$ при $1 \leq j \leq k$, то е в сила неравенството*

$$\left|\sum_{j=1}^{k} a_j\right| \leq \sum_{j=1}^{k} |a_j|.$$

Доказателство. Проверката е тривиална. □
Следващата лема съдържа известното *неравенство на Коши.*

Лема 30. *Ако* $a_j, b_j \in \mathbb{C}$ *при* $1 \le j \le k$, *то е в сила неравенството*

$$\left|\sum_{j=1}^{k} a_j b_j\right| \le \sqrt{\sum_{j=1}^{k} |a_j|^2}\,\sqrt{\sum_{j=1}^{k} |b_j|^2}.$$

Доказателство. Виж, например, [2], гл. 6, § 1. □

4.4 Леми от математическия анализ

Следната лема е известна като *преобразование на Абел.*

Лема 31. *Нека* $\{\lambda_n\}_{n=1}^{\infty}$ *е строго растяща редица,* $\lambda_n \in \mathbb{R}$, *като* $\lim_{n\to\infty} \lambda_n = \infty$ *и нека* $\{g_n\}_{n=1}^{\infty}$ *е произволна редица,* $g_n \in \mathbb{C}$. *Ако* $f(x)$ *е непрекъснато диференцируема функция в интервала* $[a, b]$, *то е в сила тъждеството*

$$\sum_{a<\lambda_n\le b} g_n\, f(\lambda_n) = -\int_a^b \left(\sum_{a<\lambda_n\le t} g_n\right) f'(t)\,dt + \left(\sum_{a<\lambda_n\le b} g_n\right) f(b).$$

Доказателство. Виж [2], гл. 1, § 3. □

Следната лема е известна като *сумационна формула на Ойлер.*

Лема 32. *Нека функцията* $f(x)$ *е непрекъснато диференцируема в интервала* $[a, b]$. *Нека* $\rho(x) = \frac{1}{2} - \{x\}$, *където* $\{x\}$ *е дробната част на* x. *Тогава е в сила тъждеството*

$$\sum_{a<n\le b} f(n) = \int_a^b f(t)\,dt + \rho(b)f(b) - \rho(a)f(a) - \int_a^b \rho(t)f'(t)\,dt.$$

Доказателство. Виж [2], гл. 1, § 1. □

Следващата лема е частен случай на известното неравенство на Бесел.

Лема 33. *Ако функцията* $f(x)$ *е интегруема в интервала* $[0, 1]$, *то за всяко* $N \in \mathbb{N}$ *е изпълнено*

$$\sum_{n=-N}^{N} \left|\int_0^1 f(\alpha)\, e(\alpha n)\, d\alpha\right|^2 \le \int_0^1 |f(\alpha)|^2\, d\alpha.$$

Доказателство. Виж [3], гл. 13, § 3. □

При $\alpha > 0$ определяме Гама-функцията на Ойлер $\Gamma(\alpha)$ чрез

$$\Gamma(\alpha) = \int_0^{\infty} t^{\alpha-1}\, e^{-t}\, dt.$$

В настоящите записки ще използваме само две от нейните свойства, които са събрани в следната

Лема 34. *При $\alpha > 0$ е в сила тъждеството*

$$\Gamma(1+\alpha) = \alpha\Gamma(\alpha).$$

При $\alpha > 0$, $\beta > 0$ е изпълнено

$$\int\limits_0^1 t^{\alpha-1} (1-t)^{\beta-1}\, dt = \frac{\Gamma(\alpha)\Gamma(\beta)}{\Gamma(\alpha+\beta)}.$$

Доказателство. Виж [3], гл. 1, § 8. □

4.5 Аритметични функции

Всяка функция $f : \mathbb{N} \to \mathbb{C}$ се нарича аритметична функция. Казваме, че една аритметична функция $f(n)$ е *мултипликативна* ако $f(1) = 1$ и ако $f(n_1 n_2) = f(n_1) f(n_2)$ винаги когато $n_1, n_2 \in \mathbb{N}, (n_1, n_2) = 1$.

Следната лема е известна като *тъждество на Ойлер.*

Лема 35. *Ако функцията $\lambda(n)$ е мултипликативна и ако редът $\sum_{q=1}^{\infty} \lambda(q)$ е абсолютно сходящ, то е в сила тъждеството*

$$\sum_{q=1}^{\infty} \lambda(q) = \prod_p \left(1 + \lambda(p) + \lambda(p^2) + \dots\right),$$

където произведението е по всички прости числа p.

Доказателство. Виж [5], гл. 17, § 4. □

4.5.1 Някои основни аритметични функции

Функция на „брой на делителите“. За всяко $n \in \mathbb{N}$ означаваме с $\tau(n)$ броят на положителните делители на n. В сила са следните леми.

Лема 36. *Функцията $\tau(n)$ е мултипликативна.*

Доказателство. Виж [1], гл. 2, § 3. □

Лема 37. *За всяко $\varepsilon > 0$ е в сила оценката*

$$\tau(n) \ll n^{\varepsilon},$$

като константата в знака на Виноградов зависи от ε.

Доказателство. Виж [1], гл. 2, зад. 11c. □

Лема 38. *Нека $X \geq 2$. Тогава за всяко $k \in \mathbb{N}$ е в сила неравенството*

$$\sum_{n \leq X} \tau^k(n) \ll X (\log X)^{2^k - 1}.$$

Доказателство. Виж [1], гл. 3, зад. 6d. □

Функция на Мьобиус. Функцията на Мьобиус $\mu(n)$ се дефинира при $n \in \mathbb{N}$ посредством формулата

$$\mu(n) = \begin{cases} 1 & \text{ако } n = 1, \\ (-1)^s & \text{ако } n \text{ е произведение на } s \text{ различни прости числа,} \\ 0 & \text{за останалите } n. \end{cases}$$

В сила са следните леми.

Лема 39. *Функцията на Мьобиус е мултипликативна.*

Доказателство. Следва директно от определението. □

Лема 40. *За всяко $n \in \mathbb{N}$ е изпълнено*

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{при } \ n = 1, \\ 0 & \text{при } \ n > 1. \end{cases}$$

Доказателство. Виж [1], гл. 2, § 4. □

Функция на Ойлер. Функцията на Ойлер $\varphi(n)$ се определя при $n \in \mathbb{N}$ като броя на естествените числа $k \le n$, за които $(k, n) = 1$. Изпълнени са следните леми.

Лема 41. *Функцията на Ойлер е мултипликативна.*

Доказателство. Виж [1], гл. 2, § 5. □

Лема 42. *При всяко $n \in \mathbb{N}$ е в сила тъждеството*

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

Доказателство. Виж [1], гл. 2, § 5. □

Лема 43. *При $n \in \mathbb{N}$ е изпълнена оценката*

$$\frac{n}{\log\log(10n)} \ll \varphi(n).$$

Доказателство. Виж [1], зад. 9g. □

Функция на Манголд. Функцията на Манголд $\Lambda(n)$ се определя при $n \in \mathbb{N}$ чрез формулата

$$\Lambda(n) = \begin{cases} \log p & \text{при } \ n = p^k, \ \text{ където } \ p \ \text{ е просто и } \ k \in \mathbb{N}; \\ 0 & \text{за останалите } \ n. \end{cases}$$

В сила е също и следната

Лема 44. *При всяко $n \in \mathbb{N}$ е изпълнено*

$$\sum_{d|n} \Lambda(d) = \log n, \qquad \Lambda(n) = \sum_{d|n} \mu(d) \log \frac{n}{d} = -\sum_{d|n} \mu(d) \log d.$$

Доказателство. Виж [4], гл. 6, § 5. □

Функция на Рамануджан. Функцията на Рамануджан $c_n(q)$ се определя при $n \in \mathbb{Z}$, $q \in \mathbb{N}$ чрез формулата

$$c_n(q) = \sum_{\substack{k=0 \\ (k,q)=1}}^{q-1} e\left(\frac{kn}{q}\right). \tag{280}$$

В сила е следната

Лема 45. *За всяко $n \in \mathbb{Z}$ функцията на Рамануджан $c_n(q)$ е мултипликативна по отношения на q и е в сила равенството*

$$c_n(q) = \frac{\mu\left(\frac{q}{(n,q)}\right)}{\varphi\left(\frac{q}{(n,q)}\right)}\varphi(q).$$

В частност, ако $(n,q) = 1$, то $c_n(q) = \mu(q)$. А при $q \mid n$ имаме $c_n(q) = \varphi(q)$.

Доказателство. Може да се намери в [5] гл. 16. □

4.6 Системи от остатъци и сравнения

Нека $n \in \mathbb{N}$. Всяка система от n на брой цели числа, които са две по две несравними по модул n, се нарича *пълна система от остатъци по модул n*. Всяка система от $\varphi(n)$ на брой цели числа, които са две по две несравними по модул n и са взаимно прости с n, се нарича *редуцирана система от остатъци по модул n*. В сила е следната лема

Лема 46. *Нека $n_1, n_2 \in \mathbb{N}$, $(n_1, n_2) = 1$. Ако a_1 пробягва пълна (редуцирана) система от остатъци по модул n_1, то числата $a_1 n_2$ образуват пълна (редуцирана) система от остатъци по модул n_1. Ако a_1 пробягва пълна (редуцирана) система от остатъци по модул n_1, а a_2 пробягва пълна (редуцирана) система от остатъци по модул n_2, то числата $a_1 n_2 + a_2 n_1$ образуват пълна (редуцирана) система от остатъци по модул $n_1 n_2$.*

Доказателство. Може да се намери в [1] гл. 3, § 4 с § 5. □

Ако $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$ то казваме, че a е сравнимо с b по модул n и пишем $a \equiv b \pmod{n}$ ако $n \mid a - b$.

Следното твърдение е доказано от Ойлер и обобщава известната *малка теорема на Ферма.*

Лема 47. *Нека $n \in \mathbb{N}$, $a \in \mathbb{N}$, като $(a, n) = 1$. Тогава е изпълнено*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Доказателство. Виж [1], гл. 3, § 6. □

Лема 48. *Нека $a, b \in \mathbb{Z}$, $a \neq 0$, $n \in \mathbb{N}$ и $(a, n) = 1$. Тогава сравнението $ax \equiv b \pmod{n}$ е разрешимо относно x.*

Доказателство. Виж [1], гл. 4, § 1. □

4.7 Показатели и примитивни корени

Нека $n \in \mathbb{N}$, $a \in \mathbb{N}$, $(a, n) = 1$. Най-малкото $\gamma \in \mathbb{N}$, за което $a^\gamma \equiv 1 \pmod n$, се нарича *показател на а по модул n.*

Лема 49. *Нека $n \in \mathbb{N}$, $a \in \mathbb{N}$, $(a, n) = 1$ и нека γ е показателят на a по модул n. Тогава ако за някое $b \in \mathbb{N}$ имаме $a^b \equiv 1 \pmod n$, то $\gamma \mid b$. В частност $\gamma \mid \varphi(n)$.*

Доказателство. Виж [1], гл. 6, § 1. □

Нека $n \in \mathbb{N}$, $n > 1$. Казваме, че g е примитивен корен по модул n ако числата $1, g, g^2, \ldots, g^{\varphi(n)-1}$ образуват редуцирана система остатъци по модул n. (Или, все едно, мултипликативната група от обратимите елементи в $\mathbb{Z}/n\mathbb{Z}$ е циклична и се поражда от g.) Ясно е, че g е примитивен корен по модул n точно когато $(g, n) = 1$ и показателят на g по модул n е равен на $\varphi(n)$.

Не за всяко n съществува примитивен корен по модул n. В сила е следната

Лема 50. *Примитивен корен по модул n съществува точно в следните случаи:*

$$n = 2, \qquad n = 4, \qquad n = p^\gamma, \qquad n = 2p^\gamma$$

където $p > 0$ е просто и $\gamma \in \mathbb{N}$.

Доказателство. Виж [1], гл. 6, § 2. □

От тази лема се вижда, че при $n = 2^\gamma$, $\gamma \geq 3$ не съществува примитивен корен по модул n. В сила е следната

Лема 51. *Ако $n = 2^\gamma$, $\gamma \geq 3$, то числото 5 притежава показател $2^{\gamma-2}$ по модул 2^γ. За всяко $m \in \mathbb{N}$, $2 \nmid m$ съществува единствена двойка числа*

$$\nu \in \{1, 2\}, \qquad \rho \in \{1, 2, \ldots, 2^{\gamma-2}\}$$

такава, че

$$m \equiv (-1)^\nu \, 5^\rho \pmod{2^\gamma}.$$

Доказателство. Виж [1], гл. 6, § 6. □

4.8 Разпределение на простите числа

Следните функции играят основна роля в теорията за разпределението на простите числа. Определяме

$$\pi(x, q, a) = \sum_{\substack{p \leq x \\ p \equiv a \pmod q}} 1, \qquad \pi(x) = \sum_{p \leq x} 1, \tag{281}$$

$$\theta(x, q, a) = \sum_{\substack{p \leq x \\ p \equiv a \pmod q}} \log p, \qquad \theta(x) = \sum_{p \leq x} \log p, \tag{282}$$

$$\psi(x, q, a) = \sum_{\substack{k \leq x \\ k \equiv a \pmod q}} \Lambda(k), \qquad \psi(x) = \sum_{k \leq x} \Lambda(k). \tag{283}$$

В следващата лема е даден важен резултат, известен като *Теорема на Чебишев за разпределението на простите числа.*

Лема 52. *При всяко* $x \in \mathbb{R}$, $x > 2$ *е изпълнено*

$$\pi(x) \asymp \frac{x}{\log x}, \qquad \theta(x) \asymp x, \qquad \psi(x) \asymp x. \tag{284}$$

Доказателство. Виж [4], гл. 7, § 2. □

В следващата лема е формулиран един класически резултат за разпределението на простите числа в аритметични прогресии, известен като *Теорема на Дирихле за простите числа в аритметични прогресии.*

Лема 53. *Ако* $a, q \in \mathbb{N}$ *са константи, за които* $(a, q) = 1$, *то*

$$\pi(x, q, a) \to \infty \qquad \text{при} \qquad x \to \infty. \tag{285}$$

Доказателство. Виж [4], гл. 10. □

Един от най-важните резултати в теорията на простите числа е следното твърдение, известно като *теорема на Зигел.*

Лема 54. *Нека* $D > 0$ *е произволна константа. Ако* $x \in \mathbb{R}$ *е достатъчно голямо, ако* $q, a \in \mathbb{N}$ *и ако* $q \leq (\log x)^D$, *то съществува* $c > 0$, *зависещо само от* D, *така че*

$$\theta(x, q, a) = \frac{x}{\varphi(q)} + O\left(x e^{-c\sqrt{\log x}}\right). \tag{286}$$

Константата в знака O *също зависи само от* D.

Доказателство. Виж [2], гл. 5, § 2. □

Забележка 1. Тази теорема е *неефективна* в смисъл, че тя не ни дава алгоритъм с който по зададено D да бъдат изчислени константата в знака O и константата c.

Забележка 2. Теоремите на Чебишев и Дирихле следват непосредствено от теоремата на Зигел.

Забележка 3. Лесно се вижда, че функцията $e^{\sqrt{\log x}}$ при $x \to \infty$ расте по-бързо от $(\log x)^A$ за произволно голяма константа $A > 0$, но по-бавно от x^ε при произволно малко $\varepsilon > 0$. Това означава, че произволно голямо $A > 0$ и за произволно малко $\varepsilon > 0$ имаме

$$x^{1-\varepsilon} \ll x e^{-c\sqrt{\log x}} \ll x(\log x)^{-A}.$$

Забележка 4. Формули, аналогични на тази в (286), са известни и за функциите $\pi(x, q, a)$ и $\psi(x, q, a)$.

Литература

[1] И.М.Виноградов, *Основы теории чисел*, Москва, „Наука", 1981.

[2] А.А.Карацуба, *Основы аналитической теории чисел*, Москва, „Наука", 1983.

[3] Е.Титчмарш, *Теория функций*, Москва, „Наука", 1980.

[4] К.Чандрасекхаран, *Введение в аналитическую теорию чисел*, Москва, „Мир", 1974.

[5] G.H.Hardy, E.M.Wright, *An introduction to the theory of numbers*, Fifth ed. Oxford Univ. Press, 1979.

[6] R.C.Vaughan, *The Hardy-Littlewood Method*, Cambridge Univ. Press, 1997.