Увод в аналитичната теория на числата – III

Д. И. Толев

Записки по едноименния изборен курс, четен от автора
във ФМИ при СУ „Св. Климент Охридски“
през зимния семестър на учебната
2012/2013 г.

София, юни 2013 г.

Съдържание

1 Увод и означения

В настоящите записки е изложен материалът от изборния курс, четен от автора във ФМИ през зимния семестър на учебната 2012/2013 г. Той е продължение на курсове, по който бяха изготвени записките *Адитивни задачи в теорията на числата*, *Увод в аналитичната теория на числата* и *Увод в аналитичната теория на числата - II*, цитирани в библиографията съответно като [6], [7] и [8]. (Файловете могат да бъде изтеглен от сайта на ФМИ). При изложението многократно ще използуваме формули, леми и теореми от [7] и ще цитираме този източник като (УАТЧ-1). Съответно записките [8] ще цитираме като (УАТЧ-2).

Във втора глава ще въведем сумите на Гаус, както и символите на Льожандър и Якоби. Ще намерим точни формули за гаусовите суми и с тяхна помощ ще докажем закона за реципрочност на квадратичните остатъци. Ще покажем също, че като се използуват формулите за сумите на Гаус, както и някои свойства на сумата на Клостерман, разгледана в (УАТЧ-2), може да се получи асимптотична формула за броя на безквадратните числа, представяни от полином от втора степен на две променливи

В трета глава се продължава изучаването на характерите на Дирихле, разгледани в (УАТЧ-1). Формулирани са понятията примитивен характер, водеш модул и др. и са изучени техните основни свойства. Въведена е сумата на Гаус, отговаряща на даден характер на Дирихле и е доказана теоремата на Пойа – Виноградов.

В четвърта глава е изложен елементарният метод на И. М. Виноградов за изследване на задачата Гаус за броя на целите точки в кръга и на задачата на Дирихле за делителите. Тези проблеми са изучавани в записките (УАТЧ-1), като там се прилага метода на експоненциалните суми. В настоящите записки се излага елементарно доказателство на теорема, която представлява вариант на Теорема 4.17 (УАТЧ-1) и по този начин се получават алтернативни доказателства на теоремите на Вороной и Серпински за остатъчните членове в задачите на Гаус и Дирихле.

Пета глава е посветена на въведение в методите на решетото. Разгледано е решетото на Ератостен – Льожандър и е обяснено защо с негова помощ не могат да бъдат получени достатъчно силни резултати. Формулирани са (без доказателство) някои от най-интересните резултати, получени чрез методите на решетото. Въведено е най-простото решето н Брун и с негова помощ е доказана теоремата на Брун за сходимостта на реда $\sum_p \frac{1}{p}$, където p пробягва простите числа, участващи в някоя двойка близнаци. Накрая е разгледано решетото на Селберг и е приложено за намиране на оценка отгоре за броя на решенията на уравнението $p_1 + p_2 = N$ в прости числа p_1, p_2.

Последната глава е посветена на метода на Шнирелман в адитивната теория на числата и на две негови приложения. Първото от тях е теоремата на Шнирелман за представяне на числата като сума от ограничен брой прости числа. Второто приложение е елементарното решение на проблема на Варинг, намерено от Хуало-Кен и Ю. Линник.

За по-подробно запознаване с разгледаните теми, а също за изучаването на други въпроси от теорията на числата, насочваме читателя към списъка от книги и статии, приложен в края на записките.

Накрая авторът изказва благодарност на Стоян Димитров и Живко Петров за посочването на някои грешки и неточности в предишните варианти на записките.

Означения

Означенията в настоящите записки до голяма степен съвпадат с означенията, възприети в (УАТЧ-1) и (УАТЧ-2), но за удобство на читателя ги привеждаме отново.

Както обикновено $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$ и $\mathbb{C}$ са множествата на естествените, целите, реалните и комплексните числа. С буквите k, l, n, m ще означаваме винаги цели числа, а буквата p ще означава просто число. Ще използуваме означенията за основните аритметични функции, въведени в (УАТЧ-1), както и техните свойства, но почти винаги ще цитираме съответните определения, леми и теореми. Когато работим със сравнения понякога ще използуваме $n \equiv a\ (q)$ като съкратен запис на $n \equiv a \pmod q$. Често ще използуваме понятията „пълна система от остатъци" и „редуцирана система от остатъци" по даден модул. Те са изяснени в Определения 3.48 и 3.49 (УАТЧ-1).

При $z \in \mathbb{C}$ ще считаме, че $\overline{z}$ е комплексно спрегнатото на z. Ако обаче разглеждаме сравнения по даден модул $q \in \mathbb{N}$ и ако числото $n \in \mathbb{Z}$ е взаимно просто с q, то $\overline{n}_{(q)}$ ще означава обратният елемент на n по модул q, т.е. число, за което $n\overline{n}_{(q)} \equiv 1 \pmod q$. Ако стойността на модула е ясна от контекста, за простота ще пишем $\overline{n}$.

Сума по естествените числа n, ненадминаващи величината x, ще означаваме накратко с $\sum_{n\le x}$. Аналогично, сума по простите числа p, ненадминаващи x, ще означаваме с $\sum_{p\le x}$. Ако $n \in \mathbb{N}$, то $\sum_{d|n}$ означава сума, в която сумирането се извършва по всички положителни делители на n и, съответно, $\sum_{p|n}$ означава сума по простите делители на n. Сумирането по числата a от някаква пълна система от остатъци по модул q ще означаваме с $\sum_{a \pmod q}$.

С буквата γ ще бележим константата на Ойлер, но понякога същата буква ще използуваме и за други цели, като точният смисъл става винаги ясен от контекста.

С $\log x$ ще означаваме натурален логаритъм на x. Както обикновено, $[x]$ и $\{x\}$ ще бъдат цялата част и съответно дробната част на x, а $||x||$ ще бъде разстоянието от x до най-близкото цяло число. Ще означаваме също $\rho(x) = \frac{1}{2} - \{x\}$ и $e(x) = e^{2\pi i x}$.

Ако за функциите $f(x)$ и $g(x)$ е изпълнено $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$ ще казваме, че те са асимптотично равни при $x \to \infty$ и ще записваме $f(x) \sim g(x)$. Ако пък имаме $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 0$, то ще записваме $f(x) = o(g(x))$. По аналогичен начин се определят горните релации и когато аргументът x клони към число.

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 $|X| \le cY$". Ако c зависи от някои други константи, например γ, δ то понякога ще отразяваме този факт, чрез означенията $X = O_{\gamma,\delta}(Y)$, съответно $X \ll_{\gamma,\delta} Y$. Ако пък константите в знаците $\ll$ или O не зависят от никакви параметри, то ще казваме, че тези константи са абсолютни. При $X \ll Y$ и $Y \ll X$ ще пишем за по-кратко $X \asymp Y$.

Буквата ε ще използуваме, за да означаваме произволно малко положително число, което не е едно и също в различни изрази. Тази уговорка ни позволява да пишем, например, $x^\varepsilon \log x \ll x^\varepsilon$. Ще считаме, че константите, включени в знаците $\ll$ и O зависят от ε, ако тази буква участва в съответните формули.

Ще използуваме $\langle x_1, \ldots, x_k \rangle$, за да означаваме наредената k-орка числа $x_1, \ldots, x_k$, докато $(x_1, \ldots, x_k)$ ще бъде най-големият общ делител на тези числа. От друга страна, (x, y) означава също отворен интервал с краища x и y, но това едва ли ще предизвика недоразумения.

Ако $\mathcal{A}$ е крайно множество, то броя на елементите му ще означаваме с $\#\mathcal{A}$. Със знака $\square$ ще бележим край на доказателство или отсъствие на такова.

2 Сума на Гаус, символи на Льожандър и Якоби и приложения

2.1 Определение на сумата на Гаус

Сумите на Гаус играят основна роля при решаване на много задачи от теорията на числата. Съществува цяла фамилия от гаусови суми и в настоящата глава разглеждаме една от тях. В следващата глава ще въведем сума на Гаус, отговаряща на даден характер на Дирихле. Значителен интерес представляват и сумите на Гаус в крайни полета, но в настоящите записки с тях няма да се занимаваме.

Определение 2.1. *Нека $q \in \mathbb{N}$, $a, b \in \mathbb{Z}$. Сума на Гаус наричаме*

$$G(q,a,b) = \sum_{x=1}^{q} e\left(\frac{ax^2+bx}{q}\right). \tag{1}$$

За простота ще означаваме също

$$G(q,a) = G(q,a,0) = \sum_{x=1}^{q} e\left(\frac{ax^2}{q}\right). \tag{2}$$

Ясно е, че сумирането в (1) и (2) може да бъде взето по коя да е пълна система от остатъци по модул q, така че бихме могли да означаваме сумирането, като използваме символа $\sum_{x \pmod q}$.

2.2 Точна формула за сумата $G(q,1)$

Както ще видим по-нататък, изчисляването на $G(q,a,b)$ се свежда до изчисляване на $G(q,1)$. Точната формула за тази сума е открита от Гаус. Ще докажем следната

Теорема 2.2 (Гаус)**.** *За произволно $q \in \mathbb{N}$ имаме*

$$G(q,1) = \frac{1+i^{-q}}{1+i^{-1}}\sqrt{q}. \tag{3}$$

Доказателство. При произволно $N \in \mathbb{N}$ разглеждаме функцията

$$D_N(u) = \sum_{k=-N}^{N} e(ku). \tag{4}$$

В сила е тъждеството

$$D_N(u) = \frac{\sin \pi(2N+1)u}{\sin \pi u}. \tag{5}$$

То се получава от (4) като приложим формулата за сума от членовете на геометрична прогресия и формулата на Ойлер

$$\sin t = \frac{e^{it} - e^{-it}}{2i}$$

(проверката на (5) оставяме на читателя). Да отбележим, че изразът в дясната страна на (5) е неопределен при $u \in \mathbb{Z}$, но можем да считаме, че неговата стойност за такива u е равна на $2N+1$, т.е. границата на $D_N(u)$ когато u клони към цяло число.

От Лема 4.9 (5) (УАТЧ-1) следва, че

$$\int_{-\frac{1}{2}}^{\frac{1}{2}} D_N(u)\,du = 1.$$

Тогава за всяко $n \in \mathbb{N}$, $n \leq q$ имаме

$$e\left(\frac{n^2}{q}\right) = I_{q,N}(n) - R_{q,N}(n), \tag{6}$$

където

$$I(n) = I_{q,N}(n) = \int_{-\frac{1}{2}}^{\frac{1}{2}} D_N(u)\, e\left(\frac{(n+u)^2}{q}\right)\, du, \tag{7}$$

$$R(n) = R_{q,N}(n) = \int_{-\frac{1}{2}}^{\frac{1}{2}} D_N(u)\, \left(e\left(\frac{(n+u)^2}{q}\right) - e\left(\frac{n^2}{q}\right)\right)\, du. \tag{8}$$

Ще оценим интеграла $R(n)$ и ще покажем, че при големи стойности на N той е пренебрежимо малък. Разбиваме го на три части

$$R(n) = J_1(n) + J_2(n) + J_3(n), \tag{9}$$

като $J_1(n)$, $J_2(n)$ и $J_3(n)$ са интеграли със същата подинтегрална функция, както в (8), но интегрирането се извършва съответно по интервалите $[-\frac{1}{2}, -\rho]$, $[-\rho, \rho]$, $[\rho, \frac{1}{2}]$, а $\rho \in (0, \frac{1}{2})$ е параметър, който ще определим по-късно.

Да разгледаме $J_3(n)$. Използуваме (5) и виждаме, че

$$J_3(n) = \int_{\rho}^{\frac{1}{2}} \frac{\sin \pi(2N+1)u}{\sin \pi u}\, \left(e\left(\frac{(n+u)^2}{q}\right) - e\left(\frac{n^2}{q}\right)\right)\, du$$

$$= \frac{-1}{\pi(2N+1)} \int_{\rho}^{\frac{1}{2}} \Phi(u)\; d\big(\cos \pi(2N+1)u\big),$$

където сме положили

$$\Phi(u) = \frac{e\left(\frac{(n+u)^2}{q}\right) - e\left(\frac{n^2}{q}\right)}{\sin \pi u}. \tag{10}$$

Сега интегрираме по части и намираме

$$J_3(n) = \frac{-1}{\pi(2N+1)} \left(\Phi(u)\Big|_{u=\rho}^{\frac{1}{2}} - \int_{\rho}^{\frac{1}{2}} \Phi'(u)\, \cos \pi(2N+1)u \; du. \right) \tag{11}$$

Да отбележим, че ако имаме комплекснозначна и непрекъснато диференцируема функция $\lambda(t)$, определена за реални $t \in [a,b]$, то е изпълнено

$$|\lambda(b) - \lambda(a)| = \left| \int_a^b \lambda'(t)\, dt \right| \leq |b-a| \max_{t\in[a,b]} |\lambda'(t)|.$$

Като приложим горната формула за функцията $e\left(\frac{t^2}{q}\right)$, определена за t от интервала с краища n, $n+u$, и използуваме, че $1 \leq n \leq q$, получаваме, че при $|u| \in \left[\rho, \frac{1}{2}\right]$ е в сила неравенството

$$\left| e\left(\frac{(n+u)^2}{q}\right) - e\left(\frac{n^2}{q}\right) \right| \ll |u|, \tag{12}$$

като константата в знака $\ll$ е абсолютна. Оттук и от (10) следва, че

$$\Phi(u) \ll 1 \qquad \text{при} \qquad \rho \leq |u| \leq \frac{1}{2} \qquad \text{и} \qquad 1 \leq n \leq q. \tag{13}$$

По-нататък, от (10) намираме

$$\Phi'(u) = 4\pi i \frac{(n+u)\, e\left(\frac{(n+u)^2}{q}\right)}{q\, \sin \pi u} - \pi \frac{\left(e\left(\frac{(n+u)^2}{q}\right) - e\left(\frac{n^2}{q}\right)\right) \cos \pi u}{\sin^2 \pi u}.$$

От тази формула и (12) следва

$$\Phi'(u) \ll \frac{1}{|u|} \qquad \text{при} \qquad \rho \leq |u| \leq \frac{1}{2} \qquad \text{и} \qquad 1 \leq n \leq q. \tag{14}$$

Заместваме оценките от (13) и (14) в (11) и получаваме

$$J_3(n) \ll \frac{1}{N} \left(1 + \int_{\rho}^{\frac{1}{2}} \frac{du}{u} \right) \ll \frac{1}{N} \log \frac{1}{\rho}. \tag{15}$$

По аналогичен начин оценяваме и $J_1(n)$ и намираме

$$J_1(n) \ll \frac{1}{N} \log \frac{1}{\rho}. \tag{16}$$

Сега да разгледаме $J_2(n)$. От (4) следва, $|D_N(u)| \leq 2N+1$ за всяко u. От това неравенство и от (12) получаваме

$$|J_2(n)| = \left| \int_{-\rho}^{\rho} D_N(u) \left(e\left(\frac{(n+u)^2}{q}\right) - e\left(\frac{n^2}{q}\right)\right) du \right| \ll N \int_{-\rho}^{\rho} |u|\, du \ll N\rho^2. \qquad (17)$$

От (9) и (15) – (17) виждаме, че

$$R(n) \ll \frac{1}{N} \log \frac{1}{\rho} + N\rho^2.$$

Полагаме $\rho = \frac{1}{2N}$ и получаваме

$$R(n) \ll \frac{\log N}{N} \qquad \text{при} \qquad 1 \leq n \leq q. \qquad (18)$$

Като просумираме равенството (6) по всички $n = 1, 2, \ldots, q$ и вземем предвид определението (2), както и оценката (18), получаваме

$$G(q,1) = H_{q,N} + O\left(\frac{q \log N}{N}\right), \qquad (19)$$

където

$$H_{q,N} = \sum_{n=1}^{q} I_{q,N}(n).$$

Сега, като се възползуваме от (4) и (7), както и от периодичността на функцията $e(t)$, намираме

$$H_{q,N} = \sum_{n=1}^{q} \int_{-\frac{1}{2}}^{\frac{1}{2}} \sum_{k=-N}^{N} e(ku)\, e\left(\frac{(n+u)^2}{q}\right) du = \sum_{n=1}^{q} \sum_{k=-N}^{N} \int_{-\frac{1}{2}}^{\frac{1}{2}} e\left(k(n+u) + \frac{(n+u)^2}{q}\right) du.$$

Извършваме смяна на променливата $n+u = v$ и получаваме

$$H_{q,N} = \sum_{n=1}^{q} \sum_{k=-N}^{N} \int_{n-\frac{1}{2}}^{n+\frac{1}{2}} e\left(kv + \frac{v^2}{q}\right) dv = \sum_{k=-N}^{N} \int_{\frac{1}{2}}^{q+\frac{1}{2}} e\left(kv + \frac{v^2}{q}\right) dv.$$

Отново сменяме променливата $v = qw$, след което допълваме получената функция на w в експонентата до точен квадрат. Получаваме

$$H_{q,N} = q \sum_{k=-N}^{N} \int_{\frac{1}{2q}}^{1+\frac{1}{2q}} e\left(q\left(w^2 + kw\right)\right) dw = q \sum_{k=-N}^{N} \int_{\frac{1}{2q}}^{1+\frac{1}{2q}} e\left(q\left(w + \frac{k}{2}\right)^2 - \frac{qk^2}{4}\right) dw$$

$$= q \sum_{k=-N}^{N} e\left(-\frac{qk^2}{4}\right) \int_{\frac{1}{2q}}^{1+\frac{1}{2q}} e\left(q\left(w + \frac{k}{2}\right)^2\right) dw.$$

За пореден път сменяме променливата $w + \frac{k}{2} = t$ и забелязваме, че

$$e\left(-\frac{qk^2}{4}\right) = \begin{cases} 1 & \text{при} \quad 2 \mid k, \\ i^{-q} & \text{при} \quad 2 \nmid k. \end{cases}$$

Получаваме

$$H_{q,N} = q\left(\Gamma_0 + i^{-q}\Gamma_1\right), \tag{20}$$

където

$$\Gamma_j = \sum_{\substack{k=-N \\ k \equiv j \pmod 2}}^{N} \int\limits_{\frac{k}{2}+\frac{1}{2q}}^{\frac{k}{2}+1+\frac{1}{2q}} e\left(qt^2\right)\, dt, \qquad j = 0, 1.$$

Оттук нататък, за улеснение на записа, ще считаме, че числото N е четно, т.е. $N = 2M$, където $M \in \mathbb{N}$. Тогава ще имаме

$$\Gamma_0 = \sum_{l=-M}^{M} \int\limits_{l+\frac{1}{2q}}^{l+1+\frac{1}{2q}} e\left(qt^2\right)\, dt = \int\limits_{-M+\frac{1}{2q}}^{M+1+\frac{1}{2q}} e\left(qt^2\right)\, dt$$

и аналогично

$$\Gamma_1 = \sum_{l=-M}^{M-1} \int\limits_{l+\frac{1}{2}+\frac{1}{2q}}^{l+\frac{3}{2}+\frac{1}{2q}} e\left(qt^2\right)\, dt = \int\limits_{-M+\frac{1}{2}+\frac{1}{2q}}^{M+\frac{1}{2}+\frac{1}{2q}} e\left(qt^2\right)\, dt.$$

Следователно при $N \to \infty$ и двете величини Γ_0, Γ_1 ще клонят към интеграла

$$\int\limits_{-\infty}^{\infty} e\left(qt^2\right)\, dt = \frac{1}{\sqrt{q}}\,\varkappa, \qquad \varkappa = \int\limits_{-\infty}^{\infty} e\left(t^2\right)\, dt,$$

(който, както е добре известно, е сходящ). Оттук и от (20) получаваме

$$\lim_{N\to\infty} H_{q,N} = \sqrt{q}\left(1 + i^{-q}\right)\varkappa.$$

Сега в равенството (19) извършваме граничен преход $N \to \infty$ и получаваме

$$G(q,1) = \sqrt{q}\left(1 + i^{-q}\right)\varkappa.$$

Като положим в горната формула $q = 1$ получаваме, че $\varkappa = (1 + i^{-1})^{-1}$, с което тъждеството (3) е доказано.

□

От Теорема 2.2 непосредствено получаваме

Следствие 2.3. *Имаме*

$$G(q,1) = \begin{cases} (1+i)\sqrt{q} & \textit{при} \quad q \equiv 0 \pmod 4, \\ \sqrt{q} & \textit{при} \quad q \equiv 1 \pmod 4, \\ 0 & \textit{при} \quad q \equiv 2 \pmod 4, \\ i\sqrt{q} & \textit{при} \quad q \equiv 3 \pmod 4. \end{cases}$$

□

2.3 Символи на Льожандър и Якоби

Първо ще определим символа на Льожандър.

Определение 2.4. *Нека $p > 2$ е просто число и $a \in \mathbb{Z}$. Казваме, че a е квадратичен остатък по модул p, ако $p \nmid a$ и ако сравнението*

$$x^2 \equiv a \pmod{p}. \tag{21}$$

е разрешимо. Казваме, че a е квадратичен неостатък по модул p, ако $p \nmid a$ и ако сравнението (21) няма решение. Определяме символа на Льожандър $\left(\frac{a}{p}\right)$, като полагаме $\left(\frac{a}{p}\right) = 0$, ако $p \mid a$, $\left(\frac{a}{p}\right) = 1$, ако a е квадратичен остатък по модул p и $\left(\frac{a}{p}\right) = -1$, ако a е квадратичен неостатък по модул p.

С помощта на символа на Льожандър може да се изрази броя на решенията на сравнението (21). В сила е следната

Лема 2.5. *Ако $p > 2$ е просто число и $a \in \mathbb{Z}$, то броят на решенията на сравнението (21) е равен на*

$$1 + \left(\frac{a}{p}\right). \tag{22}$$

Доказателство. От Лема 3.58 (УАТЧ-1) знаем, че (21) притежава най-много две решения. Ако $\left(\frac{a}{p}\right) = 1$, то (21) е разрешимо и, ако x_0 е негово решение, то очевидно и $-x_0$ е такова. Тъй като $x_0 \not\equiv -x_0 \pmod{p}$, то (21) притежава точно две решения, колкото е и стойността на израза (22). Ако $\left(\frac{a}{p}\right) = -1$, то (22) няма решение, а стойността на израза (22) е равна на 0. Ако пък $\left(\frac{a}{p}\right) = 0$, то изразът (22) има стойност 1, а сравнението (21) притежава точно едно решение, а именно $x \equiv 0 \pmod{p}$.

□

Основни свойства на символа на Льожандър са дадени в следната

Лема 2.6. *Нека $p > 2$ е просто число. Функцията на n, зададена чрез $\left(\frac{n}{p}\right)$, е периодична с период p и е напълно мултипликативна, т.е. за произволни $n_1, n_2 \in \mathbb{Z}$ е изпълнено равенството*

$$\left(\frac{n_1 n_2}{p}\right) = \left(\frac{n_1}{p}\right)\left(\frac{n_2}{p}\right). \tag{23}$$

Съществуват $\frac{1}{2}(p-1)$ на брой квадратични остатъци и също толкова на брой квадратични неостатъци по модул p.

Доказателство. Периодичността на функцията $\left(\frac{n}{p}\right)$ с период p следва непосредствено от Определение 2.4.

Ще докажем, че по модул p съществуват точно $\frac{1}{2}(p-1)$ на брой квадратични остатъци и също толкова квадратични неостатъци. Наистина, като използуваме малката теорема на Ферма (Следствие 3.54 (УАТЧ-1)), се убеждаваме, че всеки квадратичен остатък x удовлетворява сравнението $x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Това сравнение, според Лема 3.58 (УАТЧ-1), има не повече от $\frac{1}{2}(p-1)$ решения. От друга страна, числата

$$1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$$

са квадратични остатъци по модул p и, както лесно се проверява, са две по две несравними по модул p. Оттук следва, че те представляват всичките квадратични остатъци, т.е. по модул p съществуват точно $\frac{1}{2}(p-1)$ квадратични остатъци. Ясно е тогава, че квадратичните неостатъци са също толкова на брой.

Остава да докажем равенството (23) за произволни $n_1, n_2 \in \mathbb{Z}$. Ако p дели някое от числата n_1, n_2, то (23) очевидно е изпълнено. Нека сега $p \nmid n_1 n_2$.

Ако и двете числа n_1, n_2 са квадратични остатъци, то съществуват $x_1, x_2 \in \mathbb{Z}$, такива че $x_j^2 \equiv n_j \pmod{p}$, $j = 1, 2$. Тогава $(x_1 x_2)^2 \equiv n_1 n_2 \pmod{p}$, т.е. $n_1 n_2$ е квадратичен остатък и равенството (23) е изпълнено.

Нека сега едното от числата, например n_1, е квадратичен остатък, а другото — квадратичен неостатък. Тогава съществува $x \in \mathbb{Z}$, за което $x^2 \equiv n_1 \pmod{p}$. Ако допуснем, че $n_1 n_2$ е квадратичен остатък, то за някое $y \in \mathbb{Z}$ ще имаме

$$y^2 \equiv n_1 n_2 \equiv x^2 n_2 \pmod{p}.$$

Но тогава, ако $\overline{x}$ е обратният на x по модул p, ще имаме

$$(\overline{x} y)^2 \equiv n_2 \pmod{p},$$

а това противоречи на допускането, че n_2 е квадратичен неостатък.

Сега ще видим, че ако n_1 и n_2 са квадратични неостатъци, то $n_1 n_2$ е квадратичен остатък. Да допуснем противното, а именно че $n_1 n_2$ е квадратичен неостатък. Нека v пробягва всички квадратични остатъци. Тогава числата $n_1 v$ образуват система от $\frac{1}{2}(p-1)$ на брой квадратични неостатъци и са две по две несравними по модул p. Тогава $n_1 n_2$ ще е сравнимо с някое от тях по модул p, следователно за някакъв квадратичен остатък v ще имаме $n_1 n_2 \equiv n_1 v \pmod{p}$. Оттук следва, че $n_2 \equiv v \pmod{p}$ и получаваме противоречие. С това равенството (23) е доказано.

□

От горната лема непосредствено получаваме

Следствие 2.7. *Ако $p > 2$ е просто число, то*

$$\sum_{x=1}^{p} \left(\frac{x}{p}\right) = 0.$$

□

Сега ще определим символа на Якоби, който представлява обобщение на символа на Льожандър.

Определение 2.8. *Нека $q \in \mathbb{N}$, $2 \nmid q$ и нека $a \in \mathbb{Z}$. Ако $q > 1$ и $q = p_1^{l_1} \dots p_s^{l_s}$ е каноничното разлагане на q на прости множители, определяме*

$$\left(\frac{a}{q}\right) = \left(\frac{a}{p_1}\right)^{l_1} \dots \left(\frac{a}{p_s}\right)^{l_s}.$$

Считаме също, че

$$\left(\frac{a}{1}\right) = 1.$$

От горното определение и от свойствата на символа на Льожандър веднага получаваме следната

Лема 2.9. *Нека $q \in \mathbb{N}$, $2 \nmid q$ и $q > 1$. Тогава $\left(\frac{n}{q}\right)$ е напълно мултипликативна периодична с период q функция на n.*

□

2.4 Намиране на точни формули за $G(q, a, b)$

Ще започнем със следната лема, която ни показва, че е достатъчно изучаването на $G(q, n, m)$ в случая когато числата q и n са взаимно прости.

Лема 2.10. *Нека $q \in \mathbb{N}$, $a, b \in \mathbb{Z}$ и $(q, a) = d$. Тогава е в сила равенството*

$$G(q, a, b) = \begin{cases} d\, G\left(\frac{q}{d}, \frac{a}{d}, \frac{b}{d}\right) & \text{ако} \quad d \mid b, \\ 0 & \text{ако} \quad d \nmid b. \end{cases} \tag{24}$$

Доказателство. Полагаме $q = dq_1, a = da_1$. Имаме

$$G(q, a, b) = \sum_{x=1}^{q} e\left(\frac{ax^2 + bx}{q}\right) = \sum_{y=1}^{q_1} \sum_{z=0}^{d-1} e\left(\frac{da_1(y + q_1 z)^2 + b(y + q_1 z)}{dq_1}\right).$$

Тъй като функцията $e(t)$ е периодична с период 1, получаваме

$$G(q, a, b) = \sum_{y=1}^{q_1} \sum_{z=0}^{d-1} e\left(\frac{da_1 y^2 + by + bq_1 z}{dq_1}\right) = \sum_{y=1}^{q_1} e\left(\frac{a_1 y^2 + \frac{b}{d} y}{q_1}\right) \sum_{z=0}^{d-1} e\left(\frac{bz}{d}\right).$$

Като използуваме Лема 4.9 (6) (УАТЧ-1) виждаме, че сумата по z в горната формула е равна на d ако $d \mid b$ и на 0 в противен случай. Оттук следва (24) и лемата е доказана.

□

Следващата лема показва, че сумата на Гаус $G(q, a, b)$ е, в известен смисъл, мултипликативна по отношение на променливата q. По-точно, имаме

Лема 2.11. *Нека $q_1, q_2 \in \mathbb{N}$, $(q_1, q_2) = 1$, $a, b \in \mathbb{Z}$. Тогава е в сила тъждеството*

$$G(q_1q_2, a, b) = G(q_1, aq_2, b)\, G(q_2, aq_1, b). \tag{25}$$

Доказателство. Според Лема 3.52 (УАТЧ-1), ако x_1 пробягва числата $1, 2, \ldots, q_1$, а x_2 — числата $1, 2, \ldots, q_2$, то числата $x_1q_2 + x_2q_1$ образуват пълна система от остатъци по модул q_1q_2. Тогава, като използуваме също, че функцията $e(t)$ е периодична с период 1, получаваме

$$\begin{aligned} G(q_1q_2, a, b) &= \sum_{x_1=1}^{q_1} \sum_{x_2=1}^{q_2} e\left(\frac{a(x_1q_2 + x_2q_1)^2 + b(x_1q_2 + x_2q_1)}{q_1q_2}\right) \\ &= \sum_{x_1=1}^{q_1} \sum_{x_2=1}^{q_2} e\left(\frac{ax_1^2q_2^2 + ax_2^2q_1^2 + bx_1q_2 + bx_2q_1}{q_1q_2}\right) \\ &= \sum_{x_1=1}^{q_1} e\left(\frac{aq_2x_1^2 + bx_1}{q_1}\right) \sum_{x_2=1}^{q_2} e\left(\frac{aq_1x_2^2 + bx_2}{q_2}\right) \\ &= G(q_1, aq_2, b)\, G(q_2, aq_1, b). \end{aligned}$$

□

От следващата лема става ясно, че между символа на Льожандър и сумата на Гаус съществува тясна връзка.

Лема 2.12. *Нека $p > 2$ е просто число. Тогава сумата на Гаус $G(p, 1)$ се представя във вида*

$$G(p, 1) = \sum_{x=1}^{p} \left(\frac{x}{p}\right) e\left(\frac{x}{p}\right).$$

Доказателство. Имаме

$$G(p, 1) = \sum_{x=1}^{p} e\left(\frac{x^2}{p}\right) = \sum_{y=1}^{p} \sum_{\substack{x=1 \\ x^2 \equiv y \pmod p}}^{p} e\left(\frac{x^2}{p}\right) = \sum_{y=1}^{p} e\left(\frac{y}{p}\right) \sum_{\substack{x=1 \\ x^2 \equiv y \pmod p}}^{p} 1.$$

Сега, като използуваме Лема 2.5 и Лема 4.9 (6) (УАТЧ-1) получаваме

$$G(p, 1) = \sum_{y=1}^{p} e\left(\frac{y}{p}\right)\left(1 + \left(\frac{y}{p}\right)\right) = \sum_{y=1}^{p} \left(\frac{y}{p}\right) e\left(\frac{y}{p}\right).$$

□

Сега ще изчислим $G(p, a)$ при просто $p > 2$ и произволно цяло a.

Лема 2.13. *Ако $p > 2$ е просто число и $a \in \mathbb{Z}$, то е в сила тъждеството*

$$G(p, a) = \begin{cases} \left(\frac{a}{p}\right) G(p, 1) & \text{при} \quad p \nmid a, \\ p & \text{при} \quad p \mid a. \end{cases} \tag{26}$$

Доказателство. При $p \mid a$ твърдението е очевидно.

Да разгледаме случая $p \nmid a$. Работим както при доказателството на Лема 2.12 и, като използуваме също Лема 2.5, Лема 2.6 и Лема 4.9 (6) (УАТЧ-1), получаваме

$$G(p,a) = \sum_{x=1}^{p} e\left(\frac{ax^2}{p}\right) = \sum_{y=1}^{p} \sum_{\substack{x=1 \\ x^2 \equiv y \pmod p}}^{p} e\left(\frac{ax^2}{p}\right) = \sum_{y=1}^{p} e\left(\frac{ay}{p}\right) \sum_{\substack{x=1 \\ x^2 \equiv y \pmod p}}^{p} 1$$

$$= \sum_{y=1}^{p} e\left(\frac{ay}{p}\right)\left(1 + \left(\frac{y}{p}\right)\right) = \sum_{y=1}^{p-1} \left(\frac{y}{p}\right) e\left(\frac{ay}{p}\right) = \left(\frac{a}{p}\right) \sum_{y=1}^{p-1} \left(\frac{ay}{p}\right) e\left(\frac{ay}{p}\right).$$

Сумата по y в дясната страна на горното равенство е равна на $G(p,1)$ вследствие на Лема 2.12 и на факта, че ay пробягва редуцирана система от остатъци по модул p, когато y пробягва такава. С това лемата е доказана.

□

Сега ще разгледаме $G(q,1)$ в случая когато q не е непременно просто число. В сила е следната

Лема 2.14. *Нека $q \in \mathbb{N}$, $a \in \mathbb{Z}$ и $(q, 2a) = 1$. Тогава е изпълнено*

$$G(q,a) = \left(\frac{a}{q}\right) G(q,1). \tag{27}$$

Доказателство. Да разгледаме първо случая когато $q = p^k$, където $p > 2$ е просто число и $p \nmid a$. Случаят $k = 0$ е тривиален, а при $k = 1$ установихме равенството (26) от Лема 2.13, така че имаме

$$G(1,a) = 1, \qquad G(p,a) = \left(\frac{a}{p}\right) G(p,1). \tag{28}$$

Нека сега $k \geq 2$. Ясно е, че ако y и z пробягват пълни системи от остатъци по модули p^{k-1} и съответно p, то числата $y + p^{k-1}z$ образуват пълна система от остатъци по модул p^k. Тогава имаме

$$G(p^k,a) = \sum_{y=1}^{p^{k-1}} \sum_{z=1}^{p} e\left(\frac{a(y+p^{k-1}z)^2}{p^k}\right) = \sum_{y=1}^{p^{k-1}} \sum_{z=1}^{p} e\left(\frac{ay^2 + 2ayp^{k-1}z + ap^{2k-2}z^2}{p^k}\right).$$

Тъй като функцията $e(t)$ е периодична с период 1 и освен това е изпълнено $2k-2 \geq k$, получаваме

$$G(p^k,a) = \sum_{y=1}^{p^{k-1}} \sum_{z=1}^{p} e\left(\frac{ay^2 + 2ayp^{k-1}z}{p^k}\right) = \sum_{y=1}^{p^{k-1}} e\left(\frac{ay^2}{p^k}\right) \sum_{z=1}^{p} e\left(\frac{2ayz}{p}\right).$$

Според Лема 4.9 (6) (УАТЧ-1) сумата по z в дясната страна на последното равенство е равна на p, ако $p \mid y$ и на 0 в противен случай. Следователно

$$G(p^k, a) = p \sum_{\substack{y=1 \\ p \mid y}}^{p^{k-1}} e\left(\frac{ay^2}{p^k}\right) = p \sum_{x=1}^{p^{k-2}} e\left(\frac{a(px)^2}{p^k}\right) = p\, G(p^{k-2}, a). \tag{29}$$

От горната рекурентна формула и от лявото от равенствата (28) виждаме, че при $2 \mid k$ имаме

$$G(p^k, a) = p^{\frac{k}{2}} G(1, a) = p^{\frac{k}{2}}.$$

Като вземем в последното равенство $a = 1$ получаваме $G(p^k, 1) = p^{\frac{k}{2}}$. Освен това, от Определение 2.8 следва, че $\left(\frac{a}{p^k}\right) = 1$ при $2 \mid k$. Получаваме

$$G(p^k, a) = \left(\frac{a}{p^k}\right) G(p^k, 1) \qquad \text{при} \qquad 2 \mid k. \tag{30}$$

Аналогично, като използуваме рекурентната формула (29), както и дясното от равенствата (28) виждаме, че при $2 \nmid k$ е изпълнено

$$G(p^k, a) = p^{\frac{k-1}{2}} G(p, a) = p^{\frac{k-1}{2}} \left(\frac{a}{p}\right) G(p, 1).$$

От горното равенство в частност следва, че $G(p^k, 1) = p^{\frac{k-1}{2}} G(p, 1)$ и тогава намираме

$$G(p^k, a) = \left(\frac{a}{p}\right) G(p^k, 1) \qquad \text{при} \qquad 2 \nmid k. \tag{31}$$

От (30) и (31) следва, че равенството (27) е вярно когато q е степен на просто число.

Да допуснем, че (27) е изпълнено за числа q притежаващи не повече от s на брой различни прости множителя и нека имаме число q притежаващо $s+1$ на брой различни прости множителя. Представяме това число във вида $q = q'q''$, където всяко от числата q', q'' притежава не повече от s на брой различни прости множители и $(q', q'') = 1$. Тогава от Лема 2.9, Лема 2.11 и от индукционното предположение намираме

$$G(q, a) = G(q'q'', a) = G(q', aq'')\, G(q'', aq') = \left(\frac{aq''}{q'}\right) G(q', 1) \left(\frac{aq'}{q''}\right) G(q'', 1)$$

$$= \left(\frac{a}{q'}\right) \left(\frac{a}{q''}\right) \left(\frac{q''}{q'}\right) G(q', 1) \left(\frac{q'}{q''}\right) G(q'', 1)$$

От горното равенство в частност следва, че

$$G(q, 1) = \left(\frac{q''}{q'}\right) G(q', 1) \left(\frac{q'}{q''}\right) G(q'', 1)$$

и, като използуваме отново Лема 2.9, получаваме равенството (27). С това индукционната стъпка е извършена и лемата е доказана.

□

Сега ще изчислим $G(q, a, b)$ при произволно нечетно q.

Лема 2.15. *Нека $q \in \mathbb{N}$, $a, b \in \mathbb{Z}$ и $(q, 2a) = 1$. В сила е тъждеството*

$$G(q, a, b) = e\left(-\frac{\overline{(4a)}\, b^2}{q}\right)\left(\frac{a}{q}\right) G(q, 1), \tag{32}$$

където $\overline{n}$ е обратният елемент на n по модул q.

Доказателство. Имаме

$$G(q, a, b) = \sum_{x=1}^{q} e\left(\frac{ax^2 + bx}{q}\right) = \sum_{x=1}^{q} e\left(\frac{a\left(x^2 + 2\overline{(2a)}\, bx + \overline{(4a^2)}\, b^2 - \overline{(4a^2)}\, b^2\right)}{q}\right)$$

$$= e\left(-\frac{\overline{(4a)}\, b^2}{q}\right) \sum_{x=1}^{q} e\left(\frac{a\left(x + \overline{(2a)}\, b\right)^2}{q}\right)$$

$$= e\left(-\frac{\overline{(4a)}\, b^2}{q}\right)\ G(q, a),$$

тъй като $x + \overline{(2a)}\, b$ пробягва пълна система от остатъци по модул q, когато x пробягва такава. Остава да приложим (27) и получаваме равенството (32).

□

За да можем да изчисляваме $G(q, a, b)$ в общия случай е достатъчно да намерим формула за $G(2^k, a, b)$, подобна на тази от Лема 2.15. В сила е следната

Лема 2.16. *Нека $k \in \mathbb{N}$, $a, b \in \mathbb{Z}$, $2 \nmid a$.*

Ако $2 \mid b$ и $b = 2b_1$, то

$$G(2^k, a, b) = \begin{cases} 0 & \text{при} \quad k = 1, \\ e\left(-\frac{\overline{a}\, b_1^2}{2^k}\right)\ 2^{\frac{k+1}{2}}\, c(k, a) & \text{при} \quad k \geq 2, \end{cases} \tag{33}$$

където

$$c(k, a) = \begin{cases} \frac{1 + i^a}{\sqrt{2}} & \text{при} \quad 2 \mid k, \\ e\left(\frac{a}{8}\right) & \text{при} \quad 2 \nmid k. \end{cases} \tag{34}$$

Ако $2 \nmid b$, то

$$G(2^k, a, b) = \begin{cases} 2 & \text{ако} \quad k = 1, \\ 0 & \text{ако} \quad k \geq 2. \end{cases} \tag{35}$$

Доказателство. Да разгледаме случая $2 \nmid b$.

При $k = 1$ очевидно имаме

$$G(2, a, b) = \sum_{x=0}^{1} e\left(\frac{ax^2 + bx}{2}\right) = 1 + e\left(\frac{a+b}{2}\right) = 2,$$

тъй като $2 \nmid ab$.

Нека сега $k \geq 2$. Ако y и z пробягват пълни системи от остатъци съответно по модули 2^{k-1} и 2, то $y + 2^{k-1}z$ пробягва пълна система остатъци по модул 2^k. Тогава, като използуваме, че функцията $e(t)$ е периодична с период 1 и като приложим Лема 4.9 (6) (УАТЧ-1), получаваме

$$G(2^k, a, b) = \sum_{y=1}^{2^{k-1}} \sum_{z=1}^{2} e\left(\frac{a\left(y + 2^{k-1}z\right)^2 + b\left(y + 2^{k-1}z\right)}{2^k}\right)$$

$$= \sum_{y=1}^{2^{k-1}} e\left(\frac{ay^2 + by}{2^k}\right) \sum_{z=1}^{2} e\left(\frac{bz}{2}\right) = 0.$$

Да разгледаме случая $2 \mid b$, $b = 2b_1$. Имаме

$$G(2^k, a, b) = \sum_{x=1}^{2^k} e\left(\frac{ax^2 + 2b_1 x}{2^k}\right) = \sum_{x=1}^{2^k} e\left(\frac{a\left(x + \overline{a}\, b_1\right)^2 - \overline{a}\, b_1^2}{2^k}\right)$$

$$= \left(\frac{-\overline{a}\, b_1^2}{2^k}\right) G(2^k, a). \tag{36}$$

Сега остава да изчислим $G(2^k, a)$ при $2 \nmid a$.

Непосредствено се проверява, че

$$G(2, a) = 0, \qquad G(2^2, a) = 2(1 + i^a), \qquad G(2^3, a) = 4e\left(\frac{a}{8}\right) \tag{37}$$

(простата проверка оставяме на читателя). От (36) и (37) се убеждаваме във верността на (33) в случаите $k = 1, 2, 3$.

Нека сега имаме $k \geq 4$. Ако y и z пробягват пълни системо от остатъци по модули съответно 2^{k-2} и 4, то числата $y + 2^{k-2}z$ образуват пълна система от остатъци по модул 2^k. Тогава

$$G(2^k, a) = \sum_{y=1}^{2^{k-2}} \sum_{z=1}^{4} e\left(\frac{a\left(y + 2^{k-2}z\right)^2}{2^k}\right) = \sum_{y=1}^{2^{k-2}} \sum_{z=1}^{4} e\left(\frac{ay^2 + ay2^{k-1}z}{2^k}\right)$$

$$= \sum_{y=1}^{2^{k-2}} e\left(\frac{ay^2}{2^k}\right) \sum_{z=1}^{4} e\left(\frac{ayz}{2}\right).$$

От Лема 4.9 (6) (УАТЧ-1) следва, че сумата по z в последната формула има стойност 4, ако $2 \mid y$ и 0 в противен случай. Следователно

$$G(2^k, a) = 4A, \qquad \text{където} \qquad A = \sum_{\substack{y=1 \\ 2|y}}^{2^{k-2}} e\left(\frac{ay^2}{2^k}\right). \tag{38}$$

Очевидно е изпълнено

$$A = \sum_{x=1}^{2^{k-3}} e\left(\frac{ax^2}{2^{k-2}}\right). \tag{39}$$

Ще установим, че

$$A = \frac{1}{2}\, G(2^{k-2}, a). \tag{40}$$

Наистина, имаме

$$G(2^{k-2}, a) = A + B, \qquad \text{където} \qquad B = \sum_{x=2^{k-3}+1}^{2^{k-2}} e\left(\frac{ax^2}{2^{k-2}}\right)$$

и A е зададено чрез (39). Имаме

$$B = \sum_{h=1}^{2^{k-3}} e\left(\frac{a\left(2^{k-3}+h\right)^2}{2^{k-2}}\right) = \sum_{h=1}^{2^{k-3}} e\left(\frac{a\left(2^{2k-6}+2^{k-2}h+h^2\right)}{2^{k-2}}\right) = \sum_{h=1}^{2^{k-3}} e\left(\frac{ah^2}{2^{k-2}}\right) = A,$$

тъй като $k \geq 4$ и функцията $e(t)$ е периодична с период 1. От последните две равенства следва (40).

Като използуваме (38) и (40) получаваме

$$G(2^k, a) = 2G(2^{k-2}, a) \qquad \text{при} \qquad k \geq 4.$$

Тогава, като вземем предвид горната рекурентна формула и също (37) установяваме, че при $k \geq 4$ е изпълнено

$$G(2^k, a) = \begin{cases} 2^{\frac{k}{2}}\,(1+i^a) & \text{при} \quad 2 \mid k, \\ 2^{\frac{k+1}{2}}\, e\left(\frac{a}{8}\right) & \text{при} \quad 2 \nmid k. \end{cases}$$

От последната формула и от (36) заключаваме, че (33) е изпълнено и при $k \geq 4$, с което лемата е доказана.

□

Вече сме в състояние да изчисляваме сумата на Гаус $G(q, a, b)$ са произволни стойности на параметрите. Първо прилагаме Лема 2.10, за да сведем до изчисляването на сума, за която $(q, a) = 1$. След това представяме $q = 2^k q_1$, където $2 \nmid q_1$ и използуваме Лема2.11, за да сведем до изчисляване на две суми на Гаус, в първата от които числото q е нечетно, а във втората q е степен на 2. Остава да приложим Лема 2.15 и Лема 2.16.

2.5 Закон за реципрочност на квадратичните остатъци

В настоящия параграф ще видим, че от получените формули за сумите на Гаус може да се изведе закона за реципрочност на квадратичните остатъци, както и допълненията към него, отнасящи се до изчисляването на $\left(\frac{-1}{p}\right)$ и $\left(\frac{2}{p}\right)$. Ще започнем с резултатите за символа на Льожандър.

Теорема 2.17. *Ако $p > 2$ е просто число, то*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{4}} = \begin{cases} 1 & \text{при} \quad p \equiv 1 \pmod 4, \\ -1 & \text{при} \quad p \equiv 3 \pmod 4. \end{cases} \tag{41}$$

Доказателство. Като използуваме Теорема 2.2 и Лема 2.13 получаваме

$$G(p,-1) = \left(\frac{-1}{p}\right) G(p,1) = \left(\frac{-1}{p}\right) \frac{1+i^{-p}}{1+i^{-1}} \sqrt{p}$$

и също

$$G(p,-1) = \overline{G(p,1)} = \frac{1-i^{-p}}{1-i^{-1}} \sqrt{p}$$

От горните две равенства следва (41). Проверката оставяме на читателя.

□

Теорема 2.18. *Ако $p > 2$ е просто число, то*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{при} \quad p \equiv 1 \text{ или } 7 \pmod 8, \\ -1 & \text{при} \quad p \equiv 3 \text{ или } 5 \pmod 8. \end{cases} \tag{42}$$

Доказателство. Разглеждаме сумата $G(8p,1)$. От Теорема 2.2 имаме

$$G(8p,1) = \frac{1+i^{-8p}}{1+i^{-1}} \sqrt{8p} = 2\sqrt{2}(1+i)\sqrt{p}.$$

От друга страна, като приложим Теорема 2.2, Лема 2.11 и Лема 2.13 намираме

$$G(8p,1) = G(p,8)G(8,p) = \left(\frac{8}{p}\right) G(p,1)\, G(8,p) = \left(\frac{2}{p}\right) \frac{1+i^{-p}}{1+i^{-1}} \sqrt{p}\, G(8,p)$$

Лесно се вижда, че

$$G(8,p) = \sum_{x=0}^{7} e\left(\frac{px^2}{8}\right) = \begin{cases} 2\sqrt{2}(1+i) & \text{при} \quad p \equiv 1 \pmod 8, \\ 2\sqrt{2}(-1+i) & \text{при} \quad p \equiv 3 \pmod 8, \\ 2\sqrt{2}(-1-i) & \text{при} \quad p \equiv 5 \pmod 8, \\ 2\sqrt{2}(1-i) & \text{при} \quad p \equiv 7 \pmod 8. \end{cases}$$

От горните три равенства чрез прости пресмятания, които оставяме на читателя, се получава (42).

□

Следващият резултат принадлежи на Гаус.

Теорема 2.19 (Закон за реципрочност на квадратичните остатъци)**.** *Ако p_1, p_2 са нечетни прости числа, то имаме*

$$\left(\frac{p_1}{p_2}\right)\left(\frac{p_2}{p_1}\right) = (-1)^{\frac{p_1-1}{2}\cdot\frac{p_2-1}{2}} = \begin{cases} -1 & \text{при} \quad p_1 \equiv p_2 \equiv 3 \pmod 4, \\ 1 & \text{в противен случай.} \end{cases} \tag{43}$$

Доказателство. От Лема 2.11 имаме

$$G(p_1p_2, 1) = G(p_1, p_2)\, G(p_2, p_1),$$

а от Лема 2.13 и Теорема 2.2 следва

$$G(p_1, p_2) = \left(\frac{p_2}{p_1}\right) G(p_1, 1) = \left(\frac{p_2}{p_1}\right) \frac{1 + i^{-p_1}}{1 + i^{-1}} \sqrt{p_1},$$

$$G(p_2, p_1) = \left(\frac{p_1}{p_2}\right) G(p_2, 1) = \left(\frac{p_1}{p_2}\right) \frac{1 + i^{-p_2}}{1 + i^{-1}} \sqrt{p_2}.$$

От Теорема 2.2 следва също, че

$$G(p_1p_2, 1) = \frac{1 + i^{-p_1p_2}}{1 + i^{-1}} \sqrt{p_1p_2}.$$

От горните равенства получаваме

$$\frac{1 + i^{-p_1p_2}}{1 + i^{-1}} \sqrt{p_1p_2} = \left(\frac{p_2}{p_1}\right) \frac{1 + i^{-p_1}}{1 + i^{-1}} \sqrt{p_1} \ \left(\frac{p_1}{p_2}\right) \frac{1 + i^{-p_2}}{1 + i^{-1}} \sqrt{p_2},$$

откъдето

$$\left(\frac{p_1}{p_2}\right)\left(\frac{p_2}{p_1}\right) = \frac{(1 + i^{-p_1p_2})\,(1 + i^{-1})}{(1 + i^{-p_1})\,(1 + i^{-p_2})}.$$

Остава да разгледаме отделните случаи, когато простите числа са сравними с 1 или -1 по модул 4 и да се убедим, че изразът в дясната страна на горното равенство съвпада с израза в дясната страна на (43). Проверката оставяме на читателя.

□

Сега ще изведем аналози на горните твърдения за символа на Якоби. Първо ще обобщим Теорема 2.17. Имаме

Теорема 2.20. *Нека $q \in \mathbb{N}$, $2 \nmid q$ и $q > 1$. Тогава е в сила равенството*

$$\left(\frac{-1}{q}\right) = (-1)^{\frac{q-1}{2}}. \tag{44}$$

Доказателство. От Теорема 2.17 знаем, че (44) е вярно, когато q е просто число. Да допуснем, че това равенство е изпълнено за числа притежаващи не повече от s на брой прости множителя и нека имаме число q с $s+1$ прости множителя. Взимаме някакво негово разлагане $q = q_1 q_2$, където $q_1 > 1$, $q_2 > 1$. Непосредствено се проверява, че

$$\frac{q_1 - 1}{2} + \frac{q_2 - 1}{2} \equiv \frac{q - 1}{2} \pmod 2$$

и тогава, като използуваме индукционното предположение, както и Определение 2.8, получаваме

$$\left(\frac{-1}{q}\right) = \left(\frac{-1}{q_1 q_2}\right) = \left(\frac{-1}{q_1}\right)\left(\frac{-1}{q_2}\right) = (-1)^{\frac{q_1-1}{2}}(-1)^{\frac{q_2-1}{2}} = (-1)^{\frac{q_1-1}{2}+\frac{q_2-1}{2}} = (-1)^{\frac{q-1}{2}}.$$

□

Следващият резултат е обобщение на Теорема 2.18. Имаме

Теорема 2.21. *Нека $q \in \mathbb{N}$, $2 \nmid q$ и $q > 1$. Тогава е в сила равенството*

$$\left(\frac{2}{q}\right) = (-1)^{\frac{q^2-1}{8}}. \tag{45}$$

Доказателство. Разсъждаваме както при доказателството на Теорема 2.20, но сега използуваме, че ако $q = q_1 q_2$ е нечетно число, то

$$\frac{q_1^2 - 1}{8} + \frac{q_2^2 - 1}{8} \equiv \frac{q^2 - 1}{8} \pmod 2$$

(простата проверка оставяме на читателя).

□

Накрая ще дадем и обобщение на закона за реципрочност на квадратичните остатъци. Имаме

Теорема 2.22. *Нека $q_1, q_2 \in \mathbb{N}$, $2 \nmid q_1 q_1$, $q_1 > 1, q_2 > 1$. Тогава е изпълнено*

$$\left(\frac{q_1}{q_2}\right)\left(\frac{q_2}{q_1}\right) = (-1)^{\frac{q_1-1}{2}\cdot\frac{q_2-1}{2}}. \tag{46}$$

Доказателство. От Теорема 2.19 знаем, че (46) е вярно когато q_1 и q_2 са прости числа. Да допуснем верността на това равенство когато числото $q_1 q_2$ притежава не повече от s на брой прости множителя и нека са дадени q_1, q_2 такива, че $q_1 q_2$ има $s+1$ прости множителя. Нека например q_1 е съставно и $q_1 = q'q''$, където $q' > 1, q'' > 1$. Имаме

$$\left(\frac{q_1}{q_2}\right)\left(\frac{q_2}{q_1}\right) = \left(\frac{q'q''}{q_2}\right)\left(\frac{q_2}{q'q''}\right) = \left(\frac{q'}{q_2}\right)\left(\frac{q''}{q_2}\right)\left(\frac{q_2}{q'}\right)\left(\frac{q_2}{q''}\right).$$

Тогава, като използуваме индукционното предположение, получаваме

$$\left(\frac{q_1}{q_2}\right)\left(\frac{q_2}{q_1}\right) = (-1)^{\frac{q'-1}{2}\cdot\frac{q_2-1}{2}}(-1)^{\frac{q''-1}{2}\cdot\frac{q_2-1}{2}} = (-1)^{\frac{q_1-1}{2}\cdot\frac{q_2-1}{2}}$$

тъй като $\frac{q'-1}{2} + \frac{q''-1}{2} \equiv \frac{q_1-1}{2} \pmod 2$.

□

2.6 Безквадратни числа от вида $x^2 + y^2 + 1$

2.6.1 Формулировка на теоремата и някои леми

В настоящия параграф ще изследваме задача свързана с разпределението на безквадратните числа в редица, породена от полином от втора степен на две променливи.

Да разгледаме първо по-обща задача. Нека е даден полином $f(t_1, \dots, t_r)$ с цели коефициенти и с положителен старши коефициент. Да означим чрез $S_f(H)$ броя на r-орките от естествени числа $n_1, \dots, n_r \leq H$ такива, че числото $f(n_1, \dots, n_r)$ е безквадратно. Със задачата за намиране на асимптотична формула за $S_f(H)$ са се занимавали редица математици. Например, Естерман [9] през 1931 г. е разгледал полинома $f(t) = t^2 + 1$ и е доказал асимптотичната формула

$$\sum_{1 \leq x \leq H} \mu^2\left(x^2 + 1\right) = c_0 H + O\left(H^{\frac{2}{3}+\varepsilon}\right),$$

където $c_0 > 0$ е константа. Съвсем наскоро Хийт-Браун [14] подобрява оценката за остатъчния член, като замества дробта $\frac{2}{3}$ в показателя с $\frac{7}{12}$. Интересна е също съответната задача за полинома $f(t) = t(t+1)$ (виж Теорема 3.62 (УАТЧ-1), както и коментарите към нея). Известни са и много други резултати, отнасящи се до безквадратни стойности на полиноми на една или повече променливи, но на тях няма да се спираме.

В настоящата глава ще разгледаме величината $S_f(H)$ за полинома $f(t_1, t_2) = t_1^2 + t_2^2 + 1$. Означаваме

$$S(H) = \sum_{1 \leq x, y \leq H} \mu^2(x^2 + y^2 + 1). \tag{47}$$

Не е трудно да се намери асимптотична формула от вида

$$S(H) = cH^2 + O\left(H^{\frac{3}{2}+\varepsilon}\right), \tag{48}$$

където $c > 0$ е константа (точната ѝ стойност се задава чрез (54)) и $\varepsilon > 0$ е произволно малко. Ако обаче си поставим задачата да подобрим оценката за остатъчния член, срещаме по-сериозни трудности. Оказва се, че това може да бъде направено, ако използуваме резултатите за сумите на Гаус, както и свойствата на сумата на Клостерман

$$K(q, n, m) = \sum_{\substack{1 \leq x \leq q \\ (x,q)=1}} e\left(\frac{nx + m\overline{x}}{q}\right) \tag{49}$$

(както обикновено, $\overline{x}$ означава обратният елемент на x по модул q).

В записките (УАТЧ-2) видяхме, че тази сума възниква по естествен начин при изследването на различни задачи от теорията на числата. Основен резултат за сумата на Клостерман е следната теорема на А.Вейл, чието доказателство няма да привеждаме. Интересуващият се читател може да намери такова в монографията [18] на Иваниец и Ковалски.

Теорема 2.23 (А, Вейл). *За сумата на Клостерман е в сила оценката*

$$|K(q;n,m)| \leq \tau(q)\, q^{\frac{1}{2}}\, (q,n,m)^{\frac{1}{2}}.$$

□

За да подобрим оценката на остатъчния член в (48) се налага да изследваме експоненциалната сума

$$\lambda(q,n,m) = \sum_{x,\,y:\ (51)} e\left(\frac{nx+my}{q}\right), \tag{50}$$

където сумирането е по естествените числа x, y, удовлетворяващи условията

$$1 \leq x, y \leq q, \qquad x^2+y^2+1 \equiv 0 \pmod{q}. \tag{51}$$

Означаваме също

$$\lambda(q) = \lambda(q,0,0). \tag{52}$$

Оказва се, че като се използуват свойствата на сумите на Гаус, както и оценката на А.Вейл за сумата на Клостерман, може да се получи нетривиалната оценка за $\lambda(q,n,m)$, дадена в Лема 2.25. Това дава възможност да бъде доказана следната

Теорема 2.24. *За сумата $S(H)$ е в сила асимптотичната формула*

$$S(H) = cH^2 + O\left(H^{\frac{4}{3}+\varepsilon}\right), \tag{53}$$

където

$$c = \prod_p \left(1 - \frac{\lambda\,(p^2)}{p^4}\right). \tag{54}$$

Този резултат е получен неотдавна от автора [21].

Методът за доказателство на Теорема 2.24 може да се приложи за изучаване на $S_f(H)$ за произволен полином f от втора степен на две променливи. (Разбира се, тривиалните случаи, като например $f(t_1,t_2) = (t_1+t_2)^2$ трябва да бъдат изключени). При такова изследване естествено се появява величината

$$\lambda_f(q,n,m) = \sum_{\substack{1\leq x,y\leq q \\ f(x,y)\equiv 0 \pmod{q}}} e\left(\frac{nx+my}{q}\right). \tag{55}$$

Тя е тясно свързана със сумата на Клостерман и в случая $f(t_1,t_2) = t_1t_2 - 1$ сумата (55) всъщност съвпада със сумата на Клостерман. В настоящите записки обаче няма да разглеждаме тази по-обща задача.

Ще докажем следната

Лема 2.25. *Нека $q \in \mathbb{N}$, $n, m \in \mathbb{Z}$ и $8 \nmid q$. Тогава имаме*

$$|\lambda(q,n,m)| \leq 16\,\tau^2(q)\, q^{\frac{1}{2}}\, (q,n,m)^{\frac{1}{2}}. \tag{56}$$

В частност, изпълнено е

$$\lambda(q) \ll q^{1+\varepsilon}. \tag{57}$$

Забележка. Оценка от вида (56) е валидна за всяко естествено число q. Тук добавяме условието $8 \nmid q$ тъй като в този случай доказателството се опростява и понеже при доказателството на теоремата имаме нужда само от резултата на Лема 2.25.

Доказателство. Първо ще разгледаме случая $2 \nmid q$. Ясно е, че от (1), (50), (51) и от Лема 4.9 (6) (УАТЧ-1) следва

$$\lambda(q,n,m) = \sum_{1\le x,y\le q} e\left(\frac{nx+my}{q}\right) \frac{1}{q} \sum_{1\le h\le q} e\left(\frac{h(x^2+y^2+1)}{q}\right)$$

$$= \frac{1}{q} \sum_{1\le h\le q} e\left(\frac{h}{q}\right) G(q,h,n)\, G(q,h,m).$$

$$= \frac{1}{q} \sum_{l\mid q} \sum_{\substack{1\le h\le q\\(h,q)=\frac{q}{l}}} e\left(\frac{h}{q}\right) G(q,h,n)\, G(q,h,m).$$

Сега прилагаме Лема 2.10, Лема 2.15, Теорема 2.2, нашето предположение $2 \nmid q$ и определението (49). Получаваме

$$\begin{aligned}\lambda(q,n,m) &= q \sum_{\substack{l\mid q\\ \frac{q}{l}\mid(m,n)}} \frac{1}{l^2} \sum_{\substack{1\le r\le l\\(r,l)=1}} e\left(\frac{r}{l}\right) G\left(l,r,nlq^{-1}\right) G\left(l,r,mlq^{-1}\right)\\ &= q \sum_{\substack{l\mid q\\ \frac{q}{l}\mid(m,n)}} \frac{G^2(l,1)}{l^2} \sum_{\substack{1\le r\le l\\(r,l)=1}} e\left(\frac{r-\overline{(4r)}(n^2+m^2)l^2q^{-2}}{l}\right)\\ &= q \sum_{\substack{l\mid q\\ \frac{q}{l}\mid(m,n)}} \frac{(-1)^{\frac{l-1}{2}}}{l} K\left(l,1,\overline{4}(n^2+m^2)l^2q^{-2}\right).\end{aligned}$$

От последната формула и от Теорема 2.23 получаваме, че при $2 \nmid q$ имаме

$$|\lambda(q,n,m)| \le q \sum_{\substack{l\mid q\\ \frac{q}{l}\mid(m,n)}} \tau(l)\, l^{-\frac{1}{2}} \le q\,\tau(q) \sum_{r\mid(q,n,m)} q^{-\frac{1}{2}}\, r^{\frac{1}{2}} \le \tau^2(q)\, q^{\frac{1}{2}}(q,n,m)^{\frac{1}{2}}. \tag{58}$$

По-нататък, забелязваме, че функцията $\lambda(q,n,m)$ е, в известен смисъл, мултипликативна по отношение на q. По-точно, при $(q_1,q_2)=1$ е изпълнено

$$\lambda(q_1q_2,n,m) = \lambda\left(q_1, n\overline{(q_2)}_{q_1}, m\overline{(q_2)}_{q_1}\right) \lambda\left(q_2, n\overline{(q_1)}_{q_2}, m\overline{(q_1)}_{q_2}\right). \tag{59}$$

Доказателството е елементарно и го предоставяме на читателя.

Сега, ако q е произволно число, не делящо се на 8, представяме го във вида $q = 2^h q_1$, където $2 \nmid q_1$ и $h \leq 2$. Прилагаме (58), (59), както и тривиалната оценка $|\lambda(2^h, n, m)| \leq 2^{2h}$ и получаваме (56).

Накрая, ще отбележим, че (57) следва от (56) и от Лема 3.33 (УАТЧ-1).

□

Лема 2.26. *Нека $8 \nmid q$ и $D \geq 2$. Тогава за сумите*

$$U = \sum_{1 \leq n \leq D} \frac{|\lambda(q, n, 0)|}{n}, \qquad V = \sum_{1 \leq n, m \leq D} \frac{|\lambda(q, n, m)|}{n\, m}.$$

са в сила оценките

$$U \ll q^{\frac{1}{2}+\varepsilon} D^{\varepsilon}, \qquad V \ll q^{\frac{1}{2}+\varepsilon} D^{\varepsilon}, \tag{60}$$

където $\varepsilon > 0$ е произволно малко.

Доказателство. От Лема 2.25 и Лема 3.33 (УАТЧ-1) получаваме

$$U \ll q^{\frac{1}{2}+\varepsilon}\, \Sigma_0, \qquad \text{където} \qquad \Sigma_0 = \sum_{1 \leq n \leq D} \frac{(q, n)^{\frac{1}{2}}}{n}.$$

Ясно е, че

$$\Sigma_0 \ll \sum_{r \mid q} r^{\frac{1}{2}} \sum_{\substack{n \leq D \\ n \equiv 0 \pmod r}} \frac{1}{n} \ll \sum_{r \mid q} r^{-\frac{1}{2}} \sum_{m \leq \frac{D}{r}} \frac{1}{m} \ll \sum_{r \mid q} r^{-\frac{1}{2}}\, \log D \ll (qD)^{\varepsilon} \tag{61}$$

и по такъв начин установяваме първото от неравенствата (60). За да докажем и второто прилагаме отново Лема 2.25 и използуваме (61). Получаваме

$$V \ll q^{\frac{1}{2}+\varepsilon} \sum_{1 \leq n, m \leq D} \frac{(q, n, m)^{\frac{1}{2}}}{n\, m} \ll q^{\frac{1}{2}+\varepsilon} \sum_{1 \leq n, m \leq D} \frac{(q, n)^{\frac{1}{2}}}{n\, m} \ll q^{\frac{1}{2}+\varepsilon} D^{\varepsilon}.$$

□

2.6.2 Доказателство на Теорема 2.24

Използуваме тъждеството

$$\mu^2(n) = \sum_{d^2 \mid n} \mu(d)$$

(виж Лема 3.44 (УАТЧ-1)) и също (47) и записваме

$$S(H) = \sum_{x, y \leq H} \sum_{d^2 \mid x^2 + y^2 + 1} \mu(d) = \sum_{1 \leq d \leq \sqrt{2H^2+1}} \mu(d)\, T\left(H, d^2\right),$$

където $T(H, q)$ означава броя на двойките естествени числа $x, y \leq H$, удовлетворяващи сравнението $x^2 + y^2 + 1 \equiv 0 \pmod q$.

Нека z е параметър, който ще изберем по-късно. Засега считаме само, че е изпълнено

$$\sqrt{H} \leq z \leq H. \tag{62}$$

Да означим с S' приноса към $S(H)$ от събираемите, за които $z < d \leq \sqrt{2H^2+1}$. Ясно е, че

$$T\left(H, d^2\right) = \sum_{1 \leq l \leq \frac{2H^2+1}{d^2}} \sum_{\substack{1 \leq x,y \leq H \\ x^2+y^2 = ld^2-1}} 1 = \sum_{1 \leq l \leq \frac{2H^2+1}{d^2}} r(ld^2-1),$$

където $r(n)$ е броя на представянето на n като сума на два квадрата на цели числа. Но вследствие на Теорема 3.66 (УАТЧ-1) и Лема 3.33 (УАТЧ-1) имаме $r(n) \ll n^{\varepsilon}$, където $\varepsilon > 0$ е произволно малко. Тогава виждаме, че

$$T\left(H, d^2\right) \ll H^{2+\varepsilon} d^{-2}.$$

Следователно

$$S' \ll \sum_{z < d \leq \sqrt{2H^2+1}} T(H, d^2) \ll \sum_{z < d \leq \sqrt{2H^2+1}} H^{2+\varepsilon} d^{-2} \ll H^{2+\varepsilon} z^{-1},$$

а оттук получаваме

$$S(H) = \sum_{1 \leq d \leq z} \mu(d)\, T\left(H, d^2\right) + O\left(H^{2+\varepsilon} z^{-1}\right). \tag{63}$$

Оттук нататък ще считаме, че $q = d^2$, където d е безквадратно и $d \leq z$. Означаваме

$$M(H, q, x) = \sum_{\substack{h \leq H \\ h \equiv x \pmod q}} 1. \tag{64}$$

Очевидно имаме

$$M(H, q, x) = H\, q^{-1} + O\left(1\right). \tag{65}$$

Ясно е, че

$$T\left(H, q\right) = \sum_{\substack{n,m \leq H \\ n^2+m^2+1 \equiv 0 \pmod q}} 1 = \sum_{x,y:\,(51)} \sum_{\substack{n,m \leq H \\ n \equiv x \pmod q \\ m \equiv y \pmod q}} 1$$

$$= \sum_{x,y:\,(51)} M(H, q, x)\, M(H, q, y), \tag{66}$$

където сумирането по x, y е по двойките числа, удовлетворяващи (51).

Ако използуваме (63) – (66) и изберем $z = \sqrt{H}$ ще получим асимптотичната формула (48). За да установим по-точния резултат от Теорема 2.24 ще представим остатъчния член от формула (65) в явен вид. От (64) лесно се получава

$$M(H, q, y) = \left[\frac{H-y}{q}\right] - \left[\frac{-y}{q}\right] = \frac{H}{q} + \rho\left(\frac{H-y}{q}\right) - \rho\left(\frac{-y}{q}\right), \tag{67}$$

където $\rho(t) = \frac{1}{2} - \{t\}$. Заместваме последния израз за $M(H,q,y)$ в (66) и означаваме с T' приноса към $T(H,q)$, който се получава от последното събираемо от дясната страна на (67), т.е.

$$T(H,q) = \sum_{x,y:\,(51)} M(H,q,x)\ \left(\frac{H}{q} + \rho\left(\frac{H-y}{q}\right)\right) + T' \tag{68}$$

$$T' = -\sum_{x,y:\,(51)} M(H,q,x)\ \rho\left(\frac{-y}{q}\right). \tag{69}$$

Ще оценим сумата T'. За тази цел я представяме във вида

$$T' = T'' + T''', \tag{70}$$

където T'' се състои от събираемите, за които $x^2+1 \equiv 0 \pmod q$ и T''' е приносът на другите събираеми. Имаме

$$T''' = -\sum_{\substack{1\le x\le q\\ x^2+1\not\equiv 0 \pmod q}} M(H,q,x) \sum_{\substack{1\le y\le q\\ y^2\equiv -x^2-1 \pmod q}} \rho\left(\frac{-y}{q}\right) = 0 \tag{71}$$

тъй като последната сума по y е равна на нула. Наистина, в нея няма събираеми, за които $y = \frac{q}{2}$ и $y = q$. Освен това, за всяко y удовлетворяващо сравнението в сумата по y и такова, че $1 \le y < \frac{q}{2}$, числото $q-y$ удовлетворява същото сравнение и имаме

$$\rho\left(\frac{-y}{q}\right) + \rho\left(\frac{-(q-y)}{q}\right) = 0.$$

Сега да разгледаме T''. Имаме

$$T'' = -\sum_{\substack{1\le x\le q\\ x^2+1\equiv 0 \pmod q}} M(H,q,x) \sum_{\substack{1\le y\le q\\ y^2\equiv -x^2-1 \pmod q}} \rho\left(\frac{-y}{q}\right).$$

Последната сума по y е равна на $O(1)$ тъй като, според горните разсъждения, тя се редуцира до сума с най-много две събираеми (отговарящи на $y = \frac{q}{2}$ и $y = q$). Оттук и от (65) следва

$$T'' \ll \sum_{\substack{1\le x\le q\\ x^2+1\equiv 0 \pmod q}} M(H,q,x) \ll \left(Hq^{-1}+1\right)\Omega(q),$$

където $\Omega(q)$ означава броя на решенията на сравнението $x^2+1 \equiv 0 \pmod q$. Но от Лема 3.64 (УАТЧ-1) следва, че $\Omega(q) \le r(q)$, а, както отбелязахме по-горе, вследствие на Теорема 3.66 (УАТЧ-1) и Лема 3.33 (УАТЧ-1) имаме $r(q) \ll q^{\varepsilon}$. Оттук получаваме

$$T'' \ll H^{\varepsilon}\left(Hq^{-1}+1\right). \tag{72}$$

От (70) – (72) намираме

$$T' \ll H^{\varepsilon}\left(Hq^{-1}+1\right)$$

и, като вземем предвид (68) виждаме, че

$$T\left(H,q\right)=\sum_{x,y:\,(51)} M(H,q,x)\left(\frac{H}{q}+\rho\left(\frac{H-y}{q}\right)\right)+O\left(H^{\varepsilon}\left(Hq^{-1}+1\right)\right).$$

По подобен начин работим с величината $M(H,q,x)$ от горната формула и, след прости изчисления, които оставяме на читателя, намираме

$$T\left(H,q\right)=\sum_{x,y:\,(51)} \left(\frac{H}{q}+\rho\left(\frac{H-x}{q}\right)\right)\left(\frac{H}{q}+\rho\left(\frac{H-y}{q}\right)\right)+O\left(H^{\varepsilon}\left(Hq^{-1}+1\right)\right).$$

От последната формула и (50), (52) получаваме

$$T\left(H,q\right)=\frac{H^2\lambda(q)}{q^2}+2\frac{H}{q}T_1(H,q)+T_2(H,q)+O\left(H^{\varepsilon}\left(Hq^{-1}+1\right)\right), \tag{73}$$

където

$$T_1(H,q)=\sum_{x,y:\,(51)} \rho\left(\frac{H-x}{q}\right), \tag{74}$$

$$T_2(H,q)=\sum_{x,y:\,(51)} \rho\left(\frac{H-x}{q}\right)\rho\left(\frac{H-y}{q}\right). \tag{75}$$

Да разгледаме $T_1(H,q)$. Използуваме Лема 5.4 (УАТЧ-2) и записваме функцията $\rho(t)$ във вида

$$\rho(t)=\sum_{0<|n|\le H}\frac{e(nt)}{2\pi i n}+O\left(g(H,t)\right). \tag{76}$$

Тук $g(H,t)$ е положителна, безбройно много пъти диференцируема и периодична с период 1 функция на t, за която имаме представянето

$$g(H,t)=\sum_{n\in\mathbb{Z}} c_H(n)e(nt). \tag{77}$$

При това за коефициентите в горния ред на Фурие са изпълнени условията

$$c_H(n)\ll\frac{\log H}{H}\qquad\text{за всички}\qquad n\in\mathbb{Z} \tag{78}$$

и

$$\sum_{|n|\ge H^{1+\varepsilon}}|c_H(n)|\ll H^{-A}, \tag{79}$$

където $\varepsilon>0$ е произволно малко, $A>0$ е произволно голямо и константата в знака $\ll$ в последната формула зависи само от ε и A.

Използуваме горното представяне за $\rho(t)$, както и (50), и получаваме

$$T_1(H,q) = T_1'(H,q) + O\left(T_1^*(H,q)\right), \tag{80}$$

където

$$T_1'(H,q) = \sum_{x,y:\,(51)} \sum_{1\le|n|\le H} \frac{1}{2\pi i n}\, e\left(\frac{n(H-x)}{q}\right) = \sum_{1\le|n|\le H} \frac{e\left(\frac{nH}{q}\right)\,\lambda(q,-n,0)}{2\pi i n},$$

$$T_1^*(H,q) = \sum_{x,y:\,(51)} g\left(H, \frac{H-x}{q}\right). \tag{81}$$

От Лема 2.26 следва

$$T_1'(H,q) \ll H^{\varepsilon} q^{\frac{1}{2}}. \tag{82}$$

За да оценим $T_1^*(H,q)$ прилагаме Лема 2.25, Лема 2.26 и формули (50), (76) – (79) и получаваме

$$\begin{aligned} T_1^*(H,q) &= \sum_{x,y:\,(51)} \left(c_H(0) + \sum_{1\le|n|\le H^{1+\varepsilon}} c_H(n)\, e\left(\frac{n(H-x)}{q}\right)\right) + O(1) \\ &= c_H(0)\lambda(q) + \sum_{1\le|n|\le H^{1+\varepsilon}} c_H(n)\, e\left(\frac{nH}{q}\right)\,\lambda(q,-n,0) + O(1) \\ &\ll H^{\varepsilon-1}q + 1 + H^{\varepsilon-1} \sum_{1\le|n|\le H^{1+\varepsilon}} |\lambda(q,-n,0)| \\ &\ll H^{\varepsilon-1}q + 1 + H^{\varepsilon} \sum_{1\le n\le H^{1+\varepsilon}} \frac{|\lambda(q,n,0)|}{n} \\ &\ll H^{\varepsilon-1}q + H^{\varepsilon} q^{\frac{1}{2}}. \end{aligned} \tag{83}$$

От (80), (82) и (83) следва

$$T_1(H,q) \ll H^{\varepsilon-1}\, q + H^{\varepsilon}\, q^{\frac{1}{2}}. \tag{84}$$

Сега да разгледаме $T_2(H,q)$. Прилагаме Лема 2.26 и (75) – (79), (81), (83) и

получаваме

$$T_2(H,q) = \sum_{x,y:\,(51)} \sum_{1\le|n|,|m|\le H} \frac{e\left(\frac{(n+m)H}{q}\right) e\left(-\frac{nx+my}{q}\right)}{(2\pi i)^2 nm} + O\left(H^{\varepsilon} T_1^*(H,q)\right)$$

$$= \sum_{1\le|n|,|m|\le H} \frac{e\left(\frac{(n+m)H}{q}\right)}{(2\pi i)^2\, nm} \lambda(q,-n,-m) + O\left(H^{\varepsilon-1}q + H^{\varepsilon} q^{\frac{1}{2}}\right)$$

$$\ll \sum_{1\le|n|,|m|\le H} \frac{|\lambda(q,n,m)|}{|nm|} + H^{\varepsilon-1}q + H^{\varepsilon} q^{\frac{1}{2}}$$

$$\ll H^{\varepsilon-1}q + H^{\varepsilon} q^{\frac{1}{2}}. \tag{85}$$

От (73), (84) и (85) следва

$$T(H,q) = H^2 \frac{\lambda(q)}{q^2} + O\left(H^{\varepsilon}(Hq^{-\frac{1}{2}} + q^{\frac{1}{2}} + H^{-1}q)\right).$$

От горната формула, (57), (62) и (63) получаваме

$$S(H) = H^2 \sum_{1\le d\le z} \frac{\mu(d)\lambda\left(d^2\right)}{d^4} + O\left(H^{\varepsilon}\left(H + z^2 + H^{-1}z^3 + H^2 z^{-1}\right)\right)$$

$$= c\, H^2 + O\left(H^{\varepsilon}\left(H^2 z^{-1} + z^2\right)\right),$$

където

$$c = \sum_{d=1}^{\infty} \frac{\mu(d)\lambda\left(d^2\right)}{d^4}.$$

Като използуваме тъждеството на Ойлер (Теорема 3.45 (УАТЧ-1)) виждаме, че числото c, определено по-горе, съвпада със стойността на произведението (54).

Остава да изберем

$$z = H^{\frac{2}{3}}$$

и получаваме доказателство на теоремата.

□

3 Примитивни характери на Дирихле и суми на Гаус

В настоящата глава продължаваме изучаването на характерите на Дирихле, което започнахме в Глава 5.0 (УАТЧ-1). Ще определим сумата на Гаус, съответстваща на даден характер на Дирихле и ще се запознаем с основните ѝ свойства. Ще се убедим, че в някои случаи тя съвпада със сумата на Гаус, която разгледахме в предишната глава.

3.1 Примитивни характери на Дирихле

Ще започнем със следното

Определение 3.1. *Нека $k, q \in \mathbb{N}$, като $k \mid q$ и $k < q$. Нека са дадени характерите $\chi \pmod q$ и $\theta \pmod k$. Казваме, че χ е продължение на θ (или че χ се поражда от θ, или че θ поражда χ), ако за всяко $n \in \mathbb{Z}$, за което $(n, q) = 1$, е изпълнено $\chi(n) = \theta(n)$.*

Ще разгледаме няколко примера:

За всяко $q > 1$ главният характер по модул q се поражда от единствения характер по модул 1 (функцията, приемаща стойност 1 за всяко $n \in \mathbb{Z}$).

Ако $\chi_1 \pmod{12}$ е характерът, определен чрез

$$\chi_1(1) = \chi_1(5) = 1, \qquad \chi_1(7) = \chi_1(11) = -1, \qquad \chi_1(n) = 0 \quad \text{при} \quad (n, 12) > 1,$$

то χ_1 е продължение на неглавния характер $\chi^* \pmod 4$, който се определя чрез

$$\chi^*(1) = 1, \qquad \chi^*(3) = -1, \qquad \chi^*(0) = \chi^*(2) = 0.$$

Ако $\chi_2 \pmod 8$ е характерът, определен чрез

$$\chi_2(1) = \chi_1(5) = 1, \qquad \chi_2(3) = \chi_2(7) = -1, \qquad \chi_1(n) = 0 \quad \text{при} \quad (n, 2) > 1,$$

то χ_2 също се явява продължение на характера χ^*, определен по-горе.

От горните примери виждаме, че ако характерът $\chi \pmod q$ е продължение на $\theta \pmod k$, то е възможно тези две аритметични функции да съвпадат (както χ_2 и χ^*), но това не винаги е изпълнено.

По-долу, в Теорема 3.3, ще изведем необходимо и достатъчно условие характерът $\chi \pmod q$ да е продължение на някакъв характер по модул k, където $k \mid q$, $k < q$. За тази цел ще ни е нужна следната елементарна

Лема 3.2. *Нека $k, q \in \mathbb{N}$ и $k \mid q$. За всяко $a \in \mathbb{Z}$, за което $(a, k) = 1$, съществува $b \in \mathbb{Z}$ удовлетворяващо условията*

$$a \equiv b \pmod k, \qquad (b, q) = 1. \tag{86}$$

Доказателство. Като използуваме Основната теорема на аритметиката (УАТЧ-1, Теорема 3.10) представяме числото q във вида $q = q_1 q_2$, където $(q_1, k) = 1$, а q_2 е такова, че неговите прости делители са точно простите делители на k. Тогава очевидно имаме $(q_1, q_2) = 1$. Търсим числото b във вида $b = a + km$, където $m \in \mathbb{Z}$. Тогава очевидно е изпълнено сравнението в (86). Остава да изберем m така, че да е изпълнено $(a + km, q) = 1$. Очевидно последното равенство е еквивалентно на системата равенства

$$(a + km, q_1) = 1, \qquad (a + km, q_2) = 1. \tag{87}$$

Второто от тях е налице, тъй като ако допуснем, че за някое просто p е изпълнено $p \mid a + km$ и $p \mid q_2$, то ще имаме $p \mid k$, откъдето $p \mid a$, а последното противоречи на условието $(a, k) = 1$. Остава да проверим, че за някое $m \in \mathbb{Z}$ е вярно и първото от равенствата (87). За тази цел е достатъчно да установим, че сравнението

$$a + km \equiv 1 \pmod{q_1}$$

е разрешимо в цели числа m, а това е изпълнено, тъй като $(k, q_1) = 1$. (Виж Лема 3.57 (УАТЧ-1)).

□

Следващата теорема ни дава важно необходимо и достатъчно условие.

Теорема 3.3. *Нека $k, q \in \mathbb{Z}$, като $k \mid q$, $k < q$. Един характер $\chi \pmod q$ е продължение на характер по модул k точно когато за всеки $b, c \in \mathbb{Z}$, за които*

$$b \equiv c \pmod k, \qquad (bc, q) = 1, \tag{88}$$

е в сила

$$\chi(b) = \chi(c). \tag{89}$$

При това, ако съществува характер по модул k, който поражда χ, то той се определя от χ еднозначно.

Доказателство. Да допуснем, че $\theta \pmod k$ поражда $\chi \pmod q$. Ако числата b, c удовлетворяват (88), то като използуваме Определение 3.1 получаваме

$$\chi(b) = \theta(b) = \theta(c) = \chi(c),$$

или е изпълнено (89).

Сега да допуснем, че за всеки $b, c \in \mathbb{Z}$, удовлетворяващи (88), е вярно (89). Дефинираме аритметичната функция θ по следния начин.

Ако $(n, k) > 1$ полагаме $\theta(n) = 0$.

Ако $(n, k) = 1$, то като използуваме Лема 3.2, намираме число $b \in \mathbb{Z}$ такова, че $n \equiv b \pmod k$ и $(b, q) = 1$ и полагаме $\theta(n) = \chi(b)$. Тази дефиниция е коректна, тъй като ако за някое друго число $c \in \mathbb{Z}$ имаме $n \equiv c \pmod k$ и $(c, q) = 1$, то b и c ще удовлетворяват (88), откъдето ще имаме $\chi(b) = \chi(c)$.

Ще проверим, че θ е характер по модул k, като видим че са изпълнени условията от Определение 5.43 (УАТЧ-1). Първата ни задача е да установим, че за произволни $n_1, n_2 \in \mathbb{Z}$ имаме

$$\theta(n_1 n_2) = \theta(n_1)\theta(n_2). \tag{90}$$

Това равенство е очевидно, ако някое от числата n_1, n_2 не е взаимно просто с k. Нека сега имаме $(n_1 n_2, k) = 1$. Като използуваме Лема 3.2 намираме числа b_1, b_2 за които $(b_1 b_2, q) = 1$ и $n_j \equiv b_j \pmod{k}$, $j = 1, 2$. Тогава имаме също $n_1 n_2 \equiv b_1 b_2 \pmod{k}$. Като използуваме определението на θ виждаме, че $\theta(n_1 n_2) = \chi(b_1 b_2)$ и също $\theta(n_j) = \chi(b_j)$, $j = 1, 2$. Остава да използуваме, че $\chi(b_1 b_2) = \chi(b_1)\chi(b_2)$ и получаваме (90).

От определението на θ, дадено по-горе, се вижда, че $\theta(n)$ зависи само от остатъка на n по модул k, с което установяваме, че тази функция е периодична с период k.

Ако $n \in \mathbb{Z}$ и $(n, k) = 1$, то за някое b, удовлетворяващо $(b, q) = 1$, имаме

$$\theta(n) = \chi(b) \neq 0.$$

Ако пък $(n, k) > 1$, то определихме $\theta(n) = 0$.

И така, като използуваме Определение 5.43 (УАТЧ-1), виждаме, че θ е характер по модул k.

Сега ще проверим, че характерът $\chi \pmod{q}$ се поражда от $\theta \pmod{k}$. Наистина, нека вземем произволно $n \in \mathbb{Z}$, за което $(n, q) = 1$. Тъй като $k \mid q$, то ще имаме $(n, k) = 1$ и тогава, според определението на θ, ще бъде изпълнено $\theta(n) = \chi(n)$.

Остана да установим единствеността на характера по модул k, пораждащ характера $\chi \pmod{q}$. Наистина, нека $\theta^* \pmod{k}$ е характер, който също поражда χ. Да вземем произволно $n \in \mathbb{Z}$. Ако $(n, k) > 1$, то имаме

$$\theta(n) = 0 = \theta^*(n).$$

Нека сега $(n, k) = 1$. Като използуваме Лема 3.2, намираме $b \in \mathbb{Z}$, за което е изпълнено $n \equiv b \pmod{k}$ и $(b, q) = 1$. Тъй като χ се поражда както от θ, така и от θ^*, то ще имаме

$$\theta(n) = \chi(b) = \theta^*(n).$$

Тогава характерите θ и θ^* съвпадат, с което теоремата е доказана.

□

Определение 3.4. *Нека $q \in \mathbb{N}$, $q > 1$ и нека е даден характер $\chi \pmod{q}$. Казваме, че характерът χ е производен (или непримитивен), ако се поражда от характер по модул k за някое $k \mid q$, $k < q$. В противен случай казваме, че χ е примитивен. Считаме, че характерът по модул 1 (единичната функция) е примитивен.*

Да отбележим че символът на Льожандър $\left(\frac{n}{p}\right)$, където $p > 2$ е просто число, задава примитивен характер по модул p.

Ще отбележим, че в някои книги определението е малко по-различно, а именно счита се, че главните характери не са нито примитивни, нито производни. Според нашето определение, при $q > 1$ главният характер по модул q е производен, тъй като се поражда от характера по модул 1. Това малко несъответствие в терминологията обикновено не затруднява читателите.

Определение 3.5. *Нека $q \in \mathbb{N}$ и нека е даден характер $\chi \pmod q$. Водещ модул на χ наричаме най-малкото число $q^* \in \mathbb{N}$, за което $q^* \mid q$ и такова, че χ е продължение на характер $\chi^* \pmod{q^*}$, а съответно характерът χ^* [1] се нарича примитивен характер, пораждащ χ.*

От горните определения непосредствено следва

Лема 3.6. *Ако е даден характер $\chi \pmod q$ с водещ модул q^* и ако $\chi^* \pmod{q^*}$ е съответният примитивен характер, а χ_0 е главният характер по модул q, то*

$$\chi(n) = \chi_0(n)\chi^*(n) \qquad \text{за всяко} \qquad n \in \mathbb{Z}. \tag{91}$$

□

В следващата теорема е дадено необходимо и достатъчно условие за примитивност на даден характер.

Теорема 3.7. *Нека $q \in \mathbb{N}$, $q > 1$ и нека е даден характер $\chi \pmod q$. Тогава следните две условия са еквивалентни:*

(*A*) *Характерът χ е примитивен.*

(*B*) *За всяко $k \in \mathbb{N}$, за което $k \mid q$, $k < q$, съществува $m \in \mathbb{Z}$ такова, че*

$$(m, q) = 1, \qquad m \equiv 1 \pmod k, \qquad \chi(m) \neq 1. \tag{92}$$

Доказателство. Да допуснем, че е вярно (*A*), но не е изпълнено (*B*). Тогава съществува естествено число $k \mid q$, $k < q$ такова, че за всяко $m \in \mathbb{Z}$, удовлетворяващо $(m, q) = 1$ и $m \equiv 1 \pmod k$, имаме $\chi(m) = 1$.

Вземаме $b, c \in \mathbb{Z}$, за които са изпълнени условията (88) от Теорема 3.3. Тъй като $(c, q) = 1$, то съществува $h \in \mathbb{Z}$, за което $hc \equiv 1 \pmod q$ (виж Лема 3.57 (УАТЧ-1)). Но тогава ще имаме $(hc, q) = 1$ и $hc \equiv 1 \pmod k$, следователно

$$\chi(h)\chi(c) = \chi(hc) = 1.$$

От друга страна, от (88) следва $(hb, q) = 1$ и $hb \equiv 1 \pmod k$, откъдето

$$\chi(h)\chi(b) = \chi(hb) = 1.$$

[1] Характерът χ^* е примитивен, тъй като ако е продължение на характер $\theta \pmod k$, където $k \mid q^*$, $k < q^*$, то и χ ще е продължение на θ.

Но тогава $\chi(h)\chi(b) = \chi(h)\chi(c)$ и понеже $\chi(h) \neq 0$ ще имаме $\chi(b) = \chi(c)$, Сега, като използуваме Теорема 3.3, заключаваме, че съществува характер по модул k, който поражда χ. Но това противоречи на допускането, че χ е примитивен. Или от условието (A) следва (B).

Сега да допуснем, че е изпълнено (B), но не е вярно (A). Тогава характерът χ е производен, т.е. той е продължение на характер $\theta \pmod k$ за някое $k \mid q$, $k < q$. Следователно, ако вземем произволно $m \in \mathbb{Z}$, удовлетворяващо първите две условия от (92), ще имаме $\chi(m) = \theta(m) = 1$. Това обаче противоречи на условието (B), за което допуснахме, че е изпълнено. Изводът е, че от (B) следва (A), с което теоремата е доказана.

□

3.2 Сума на Гаус, отговаряща на даден характер на Дирихле

Ще определим сума на Гаус, отговаряща на даден характер, и ще изучим някои от свойствата ѝ. Чрез $\sum_{a \pmod q}$ ще означаваме сума по променливата a, пробягваща произволна пълна система от остатъци по модул q. Ще използуваме това означение само в случаите, когато изборът на конкретната система е без значение за стойността на сумата.

Определение 3.8. *Нека $m \in \mathbb{Z}, q \in \mathbb{N}$ и нека е даден характер $\chi \pmod q$. Величината*

$$G(m,\chi) = \sum_{a \pmod q} \chi(a) e\left(\frac{am}{q}\right), \tag{93}$$

се нарича сума на Гаус. Определяме също

$$\tau(\chi) = G(1,\chi) = \sum_{a \pmod q} \chi(a) e\left(\frac{a}{q}\right). \tag{94}$$

Да отбележим, че функциите $\chi(a)$ и $e\left(\frac{am}{q}\right)$ са периодични с период q, следователно изборът на пълната система от остатъци, която пробягва a, не оказва влияние върху стойността на сумата на Гаус.

Връзка между величините $G(m,\chi)$ и $\tau(\chi)$ е дадена в следната

Лема 3.9. *Ако е даден характерът $\chi \pmod q$ и ако $(m,q) = 1$, то*

$$G(m,\chi) = \overline{\chi}(m)\tau(\chi). \tag{95}$$

Доказателство. Тъй като $(m,q) = 1$, то $1 = |\chi(m)|^2 = \chi(m)\overline{\chi(m)}$. Следователно

$$G(m,\chi) = \sum_{a \pmod q} \chi(m)\,\overline{\chi(m)}\,\chi(a)\,e\left(\frac{am}{q}\right) = \overline{\chi}(m) \sum_{a \pmod q} \chi(am)\,e\left(\frac{am}{q}\right).$$

Но когато a пробягва пълна система от остатъци по модул q, то am също пробягва такава система. Следователно сумата в дясната страна на горния израз е равна на $\tau(\chi)$, с което (95) е доказано.

□

Лема 3.9 дава възможност стойността на характера χ да се изрази чрез съответната сума на Гаус. Съществен недостатък на този резултат е, че тъждеството (95) е вярно при условията, че $q > 1$ и $(m, q) = 1$. Без тези условия тъждеството може и да не е изпълнено. Наистина, ако χ е главният характер по модул q и $m = 0$, то изразът в лявата страна на (95) е равен на $\varphi(q)$, а от дясната страна имаме 0. Следващата важна теорема ни показва, че указаният недостатък може да бъде отстранен, ако нашият характер е примитивен.

Теорема 3.10. *Ако характерът $\chi \pmod q$ е примитивен, то равенството (95) е вярно за всяко $m \in \mathbb{Z}$.*

Доказателство. Случаят $(m, q) = 1$ вече е разгледан в Лема 3.9 и оттук нататък ще считаме, че $(m, q) > 1$. Тъй като в този случай имаме $\overline{\chi}(m) = 0$, то за да проверим равенството (95) остава да докажем, че

$$G(m, \chi) = 0. \tag{96}$$

Полагаме

$$d = (m, q), \qquad m = dm_1, \qquad q = dq_1 \tag{97}$$

и тогава от (93) следва

$$G(m, \chi) = \sum_{a \pmod{dq_1}} \chi(a) e\left(\frac{am_1}{q_1}\right).$$

За да получим пълна система от остатъци по модул dq_1 е достатъчно да вземем числата $bq_1 + c$, където b пробягва пълна система от остатъци по модул d, а c — пълна система от остатъци по модул q_1. (Простото доказателството на този факт предоставяме на читателя). Тогава, като използуваме елементарните свойства на функцията $e(t)$ (виж Лема 4.9 (УАТЧ-1)), получаваме

$$G(m, \chi) = \sum_{b \pmod d} \sum_{c \pmod{q_1}} \chi(bq_1 + c)\, e\left(\frac{(bq_1 + c)m_1}{q_1}\right)$$

$$= \sum_{c \pmod{q_1}} e\left(\frac{cm_1}{q_1}\right) F(c), \tag{98}$$

където

$$F(c) = \sum_{b \pmod d} \chi(bq_1 + c). \tag{99}$$

Да отбележим, че тъй като χ е периодична функция с период q, то в горната сума е без значение коя пълна система от остатъци по модул d пробягва сумационната променлива b. Освен това имаме

$$F(c) = F(c') \qquad \text{при} \qquad c \equiv c' \pmod{q_1}. \tag{100}$$

Наистина, ако например $c' = c + kq_1$ за някое $k \in \mathbb{Z}$, то

$$F(c') = \sum_{b \pmod{d}} \chi(bq_1 + c + kq_1) = \sum_{b \pmod{d}} \chi((b+k)q_1 + c) = F(c),$$

тъй като $b + k$ пробягва пълна система от остатъци по модул q_1, когато b пробягва такава.

Ние разглеждаме случая $d > 1$ и поради това ще имаме $q_1 < q$. Но по условие характерът χ е примитивен и тогава, като използуваме Теорема 3.7, заключаваме, че съществува $h \in \mathbb{Z}$, за което

$$(h, q) = 1, \qquad h \equiv 1 \pmod{q_1}, \qquad \chi(h) \neq 1. \tag{101}$$

Оттук и от (99) намираме

$$\chi(h)F(c) = \chi(h) \sum_{b \pmod{d}} \chi(bq_1 + c) = \sum_{b \pmod{d}} \chi(hbq_1 + hc). \tag{102}$$

Но от първото условие в (101) и от това, че $d \mid q$ имаме $(h, d) = 1$. Тогава hb пробягва пълна система от остатъци по модул d, когато b пробягва такава, откъдето следва, че сумата в дясната страна на (102) е равна на $F(hc)$. Но от сравнението в (101) следва, че $hc \equiv c \pmod{q_1}$ и тогава според (100) имаме $F(hc) = F(c)$. И така, получаваме

$$\chi(h)F(c) = F(c).$$

Оттук, като използуваме третото условие от (101), заключаваме, че $F(c) = 0$. Остава да заместим получената стойност в (98) и установяваме (96). С това теоремата е доказана.

□

С помощта на резултата от Теорема 3.10 не е трудно да се изчисли модула на сумата на Гаус $\tau(\chi)$, отговаряща на примитивен характер. В сила е следната

Теорема 3.11. *Ако е даден примитивен характер $\chi \pmod{q}$ и ако $\tau(\chi)$ е определено чрез* (94)*, то*

$$|\tau(\chi)| = \sqrt{q}. \tag{103}$$

Доказателство. От равенството (95), което е вярно за всяко $m \in \mathbb{Z}$, при условие, че χ е примитивен, получаваме

$$|G(m, \chi)|^2 = |\overline{\chi}(m)|^2 \, |\tau(\chi)|^2 = \begin{cases} |\tau(\chi)|^2 & \text{ако} \quad (m, q) = 1, \\ 0 & \text{ако} \quad (m, q) > 1. \end{cases}$$

Сега, като сумираме горното равенство по всички m от някаква пълна ситема от остатъци по модул q и означим

$$\Gamma = \sum_{m \pmod q} |G(m,\chi)|^2 ,$$

то според определението на функцията на Ойлер (виж Определение 3.20 (УАТЧ-1)), ще получим

$$\Gamma = |\tau(\chi)|^2 \varphi(q). \tag{104}$$

От друга страна, като използуваме определението (93), виждаме, че

$$\begin{aligned}
\Gamma &= \sum_{m \pmod q} G(m,\chi)\,\overline{G(m,\chi)} \\
&= \sum_{m \pmod q} \sum_{a \pmod q} \chi(a)\, e\left(\frac{am}{q}\right) \sum_{b \pmod q} \overline{\chi}(b)\, e\left(\frac{-bm}{q}\right) \\
&= \sum_{a \pmod q} \sum_{b \pmod q} \chi(a)\,\overline{\chi}(b) \sum_{m \pmod q} e\left(\frac{(a-b)m}{q}\right).
\end{aligned}$$

Сумата по m в горния израз е равна на q при $a \equiv b \pmod q$ и на 0 в противен случай (виж Лема 4.9 (6) (УАТЧ-1)). Тогава имаме

$$\Gamma = q \sum_{a \pmod q} \sum_{\substack{b \pmod q \\ a \equiv b \pmod q}} \chi(a)\,\overline{\chi}(b) = q \sum_{a \pmod q} |\chi(a)|^2 = q \sum_{\substack{a \pmod q \\ (a,q)=1}} 1 = q\,\varphi(q).$$

Като сравним горната формула за Γ с равенството (104), получаваме

$$|\tau(\chi)|^2 = q,$$

с което доказателството на (103) е завършено.

□

3.3 Неравенство на Пойа-Виноградов

Получените резултати имат многобройни приложения. Един от тях е неравенството на Пойа-Виноградов, изложено в следващата теорема. То представлява съществено подобрение на елементарната оценка за сума от стойностите на неглавен характер, когато аргументът пробягва даден интервал (виж (УАТЧ-1), Теорема 5.44, (7) и също Лема 5.15). Условието е характерът да е примитивен, но както ще видим по-долу, подобен резултат може да се докаже за произволен неглавен характер.

Теорема 3.12 (Пойа, Виноградов)**.** *Нека $q \in \mathbb{N}$, $q > 1$ и нека е даден примитивен характер $\chi \pmod q$. Ако са дадени произволни $y, z \in \mathbb{R}$, $y < z$ и ако*

$$S = \sum_{y < n \le z} \chi(n), \tag{105}$$

то е в сила неравенството

$$|S| \ll \sqrt{q}\,\log q, \tag{106}$$

като константата в знака $\ll$ *е абсолютна.*

Доказателство. Знаем, че за произволно $w \in \mathbb{R}$ е изпълнено

$$\sum_{w<n\leq w+q} \chi(n) = 0$$

(виж (УАТЧ-1), Теорема 5.44 (6)). Поради това, можем да считаме, че

$$z - y < q. \tag{107}$$

Да отбележим, че тъй като характерът χ е примитивен, то и неговият комплексно-спрегнат $\overline{\chi}$ е такъв (елементарната проверка оставяме на читателя). Тогава, като използуваме Теорема 3.11 виждаме, че

$$|\tau(\overline{\chi})| = \sqrt{q}. \tag{108}$$

По-нататък, от Теорема 3.10 следва, че за всяко $n \in \mathbb{N}$ е изпълнено

$$\chi(n) = \frac{G(n,\overline{\chi})}{\tau\,(\overline{\chi})}.$$

Заместваме последния израз в (105) и, като вземем предвид определението (93), получаваме

$$S = \tau(\overline{\chi})^{-1} \sum_{y<n\leq z} G(n,\overline{\chi}) = \tau(\overline{\chi})^{-1} \sum_{y<n\leq z} \sum_{a \pmod q} \overline{\chi}(a)\, e\left(\frac{an}{q}\right)$$

За нашите изчисления е по-удобно, ако оставим сумационната променлива a да пробягва целите числа от интервала $\left(-\frac{q}{2}, \frac{q}{2}\right]$. Тогава, като сменим реда на сумиране, намираме

$$S = \tau(\overline{\chi})^{-1} \sum_{-\frac{q}{2}<a\leq\frac{q}{2}} \overline{\chi}(a) \sum_{y<n\leq z} e\left(\frac{an}{q}\right),$$

след което използуваме (108) и неравенството на триъгълника и получаваме

$$|S| \leq q^{-\frac{1}{2}} \sum_{-\frac{q}{2}<a\leq\frac{q}{2}} \left|\sum_{y<n\leq z} e\left(\frac{an}{q}\right)\right|.$$

Сумата по n в горния израз представлява сума от членовете на геометрична прогресия и може да се изрази в явен вид, след което да се оцени. Точната формулировка на съответния резултат, както и подробните изчисления са дадени в (УАТЧ-1), Лема 4.10. Като използуваме тази лема и (107) виждаме, че

$$\left|\sum_{y<n\leq z} e\left(\frac{an}{q}\right)\right| \leq \min\left(q, \frac{1}{||\frac{a}{q}||}\right).$$

(Както обикновено, $||t||$ означава разстоятието от t до най-близкото цяло число. Считаме също, че $\min\left(q, \frac{1}{0}\right) = q$).

Но очевидно при $|a| \leq \frac{q}{2}$ имаме $||\frac{a}{q}|| = |\frac{a}{q}|$. Тогава от горните оценки и от позната формула за частичните суми на хармоничния ред (виж (УАТЧ-1), Лема 2.6 (3)) получаваме

$$|S| \leq q^{-\frac{1}{2}} \sum_{-\frac{q}{2}<a\leq\frac{q}{2}} \min\left(q, \frac{q}{|a|}\right) \leq \sqrt{q}\left(1 + 2\sum_{1\leq a\leq\frac{q}{2}} \frac{1}{a}\right) \ll \sqrt{q}\,\log q.$$

□

Сега ще получим резултат, подобен на този от Теорема 3.12, но вече за произволен неглавен характер. В сила е следната

Теорема 3.13. *Нека $\chi \pmod q$ е неглавен характер с водещ модул q^*. Ако са дадени произволни $y, z \in \mathbb{R}$, $y < z$ ако*

$$S = \sum_{y<n\leq z} \chi(n), \tag{109}$$

то е в сила неравенството

$$|S| \ll \tau(q)\,\sqrt{q^*}\,\log q^*, \tag{110}$$

където $\tau(q)$ е броят на положителните делители на q, а константата в знака $\ll$ е абсолютна.

Доказателство. Използуваме Лема 3.6 и представяме χ във вида (91), където $\chi^* \pmod{q^*}$ е примитивен характер и χ_0 е главният характер по модул q. Тогава, като използуваме определението на главен характер (виж (УАТЧ-1), Определение 5.43) и основното свойство на функцията на Мьобиус (виж (УАТЧ-1), Определение 3.19 и Лема 3.34), получаваме

$$S = \sum_{y<n\leq z} \chi_0(n)\,\chi^*(n) = \sum_{\substack{y<n\leq z\\(n,q)=1}} \chi^*(n) = \sum_{y<n\leq z} \chi^*(n) \sum_{d|(n,q)} \mu(d).$$

Сега сменяме реда на сумиране и намираме

$$S = \sum_{d|q} \mu(d) \sum_{\substack{y<n\leq z\\ n\equiv 0 \pmod d}} \chi^*(n) = \sum_{d|q} \mu(d) \sum_{\frac{y}{d}<m\leq\frac{z}{d}} \chi^*(md) = \sum_{d|q} \mu(d)\chi^*(d) \sum_{\frac{y}{d}<m\leq\frac{z}{d}} \chi^*(m).$$

Остава да приложим неравенството на триъгълника и Теорема 3.12 и виждаме, че

$$|S| \leq \sum_{d|q} \left| \sum_{\frac{y}{d}<m\leq\frac{z}{d}} \chi^*(m) \right| \ll \sqrt{q^*}\,\log q^* \sum_{d|q} 1,$$

с което доказателството на (110) е завършено.

□

4 Елементарен метод на И. М. Виноградов в задачите за целите точки

4.1 Формулировка на теоремата и нейни приложения

В Глава 4 на (УАТЧ-1) разгледахме задачата на Гаус за броя целите точки в кръга и задачата на Дирихле за броя на целите точки под хиперболата. Ще припомним техните формулировки.

Задачата на Гаус се състои в намирането на възможно най-точна асимптотична формула за величината

$$K(R) = \#\{\langle n, m\rangle \in \mathbb{Z}^2 \ : \ n^2 + m^2 \leq R\},$$

която представлява броя на точките с целочислени координати в кръг с радиус $\sqrt{R}$. Лесно се съобразява, че главният член в предполагаемата асимптотична формула е πR, т.е. лицето на съответния кръг. Следователно, ако определим $\Delta_K(R)$ чрез формулата

$$K(R) = \pi R + \Delta_K(R),$$

то задачата се свежда до намирането на възможно най-добра оценка за остатъчния член $\Delta_K(R)$. Гаус, с помощта на елементарни разсъждения, е установил, че

$$\Delta_K(R) = O\left(\sqrt{R}\right).$$

(Простото доказателство на тази оценка е приведено в Теорема 4.1 (УАТЧ-1)).

Съответно, задачата на Дирихле се състои в намирането на възможно най-точна асимптотична формула за величината

$$L(R) = \#\{\langle n, m\rangle \in \mathbb{N}^2 \ : \ nm \leq R\},$$

която ни дава броя на точките с целочислени координати от първи квадрант, лежащи под или върху хиперболата $xy = R$. Лесно се съобразява също, че

$$L(R) = \sum_{n \leq R} \tau(n),$$

където $\tau(n)$ е броят на положителните делители на N, поради което тази задача е известна още като *задача на Дирихле за делителите*. Дирихле е установил, че

$$L(R) = R \log R + (2\gamma - 1)R + \Delta_L(R),$$

където γ означава константата на Ойлер, а за остатъчния член е изпълнено

$$\Delta_L(R) = O\left(\sqrt{R}\right).$$

Доказателство на последната оценка е приведено в края на параграф 4.5 (УАТЧ-1).

В Глава 4 (УАТЧ-1) е показано, че по-точното оценяване на остатъчните членове в задачите на Гаус и на Дирихле се свежда до намирането на нетривиални оценки на суми от вида

$$T = \sum_{a<n\leq b} \rho(f(n)), \tag{111}$$

където $\rho(x) = \frac{1}{2} - \{x\}$, а $f(x)$ е реалнозначна функция, дефинирана в интервала $[a, b]$. С помощта на метода на експоненциалните суми е доказана Теорема 4.17 (УАТЧ-1), в която, грубо казано, се твърди, че ако втората производна на $f(x)$ е „малка", но не „прекалено малка" в целия интервал $[a, b]$, то сумата T може да се оцени нетривиално. Този резултат дава възможност да бъдат доказани следните оценки на Вороной и Серпински:

$$\Delta_K(R) = O\left(R^{\frac{1}{3}} \log R\right), \qquad \Delta_L(R) = O\left(R^{\frac{1}{3}} \log^2 R\right) \tag{112}$$

(теореми 4.2 и 4.5 (УАТЧ-1)).

През 1917 г. И. М. Виноградов открива елементарен метод за оценяване на суми от вида (111) и по такъв начин намира нови доказателства на оценките (112). В настоящата глава ще изложим метода на Виноградов и ще докажем следната теорема, която представлява вариант на Теорема 4.17 (УАТЧ-1).

Теорема 4.1. *Нека функцията $f(x)$ е реалнозначна и два пъти непрекъснато диференцируема в $[a, b]$, нека $a, b, \mu, \rho \in \mathbb{R}$,*

$$b - a \geq 10, \qquad \mu \geq 1, \qquad \rho > 0, \tag{113}$$

като

$$\rho \leq |f''(x)| \leq \mu\rho \qquad \textit{при} \qquad x \in [a, b]. \tag{114}$$

Тогава за сумата T, определена от (111)*, е в сила оценката*

$$T \ll \left(\mu^2(b-a)\rho^{\frac{1}{3}} + \mu\rho^{-\frac{2}{3}}\right) \log\left(\rho^{-1} + 2\right), \tag{115}$$

като константата в знака $\ll$ е абсолютна.

Както е отбелязано след формулировката на Теорема 4.17 (УАТЧ-1), обикновено в приложенията параметърът μ е константа. Поради това е без значение фактът, че в дясната страна на (115) параметърът μ участва с по-висока степен, отколкото в оценката от Теорема 4.17 (УАТЧ-1). По-съществена слабост на оценката (115) е, че събираемото $\mu\rho^{-\frac{2}{3}}$ от израза в скобите от дясната страна на (115) е по-голямо (поне в нетривиалния случай $\rho < 1$) от съответното събираемо $\rho^{-\frac{1}{2}}$ в оценката от Теорема 4.17 (УАТЧ-1). Това обаче, както ще видим по-долу, не възпрепятства получаването на оценките (112).

Наистина, ако следваме разсъжденията, изложени в параграф 4.9 (УАТЧ-1), но използуваме Теорема 4.1, ще видим, че предпоследната формула в този параграф трябва да се замени с

$$\Delta_K^*(R) \ll \left(R^{\frac{1}{2}}\left(R^{-\frac{1}{2}}\right)^{\frac{1}{3}} + \left(R^{-\frac{1}{2}}\right)^{-\frac{2}{3}}\right) \log R \ll R^{\frac{1}{3}} \log R.$$

Оттук се получава първата оценка от (112).

Аналогично, в разсъжденията, изложени в параграф 4.10 (УАТЧ-1), предпоследната формула трябва да бъде заменена с

$$\Delta_i \ll \left(R^{\frac{1}{2}} 2^{-i} \left(2^{3i-2} R^{-\frac{1}{2}} \right)^{\frac{1}{3}} + \left(2^{3i-2} R^{-\frac{1}{2}} \right)^{-\frac{2}{3}} \right) \log R \ll R^{\frac{1}{3}} \log R$$

и оттук следва втората оценка от (112).

4.2 Помощни резултати

Нека е дадена сумата

$$S_0 = \sum_{n=0}^{q-1} \rho \left(\frac{an+b}{q} \right),$$

където $q \in \mathbb{N}$, $a, b \in \mathbb{Z}$, $(a,q) = 1$. Като използуваме определението на функцията $\rho(t)$ и факта, че $an+b$ пробягва пълна система от остатъци по модул q, когато n пробягва такава, лесно се вижда, че $S_0 = \frac{1}{2}$. Простите изчисления оставяме на читателя. Оказва се, че ако параметърът b зависи от n, но не се изменя твърде много, когато n пробягва числата $0, 1, \ldots, q-1$, то съответната сума отново по модул е сравнително малка. По-точно, в сила е следната

Лема 4.2. *Нека $\kappa, h \in \mathbb{R}$, $h \geq 0$, $q \in \mathbb{N}$, $a \in \mathbb{Z}$, $(a,q) = 1$. Нека за всяко $n = 0, 1, \ldots, q-1$ е определено $\xi(n) \in \mathbb{R}$, като*

$$\kappa \leq \xi(n) \leq \kappa + h \qquad \textit{при} \qquad n = 0, 1, \ldots, q-1. \tag{116}$$

Тогава за сумата

$$S = \sum_{n=0}^{q-1} \rho \left(\frac{an + \xi(n)}{q} \right)$$

е изпълнено

$$|S| \leq 2h + 3. \tag{117}$$

Доказателство. Полагаме

$$b = [\kappa], \qquad \eta = \{\kappa\} \tag{118}$$

и записваме S във вида

$$S = \sum_{n=0}^{q-1} \rho \left(\frac{an + b + \xi_1(n)}{q} \right),$$

където $\xi_1(n) = \xi(n) - b$. Ясно е, че от (116) следва

$$\eta \leq \xi_1(n) \leq \eta + h \qquad \text{при} \qquad n = 0, 1, \ldots, q-1. \tag{119}$$

От Лема 3,51 (УАТЧ-1) знаем, че числата

$$an + b, \qquad n = 0, 1, \ldots, q-1 \tag{120}$$

образуват пълна система остатъци по модул q. Следователно

$$S = \sum_{k=0}^{q-1} \rho\left(\frac{k+\xi_2(k)}{q}\right), \tag{121}$$

където $\xi_2(k) = \xi_1(n_k)$, а n_k е това от числата $0, 1, \ldots, q-1$, за което е изпълнено $an_k + b \equiv k \pmod q$. При това, от (119) следва

$$\eta \le \xi_2(k) \le \eta + h \qquad \text{за} \qquad k = 0, 1, \ldots, q-1. \tag{122}$$

Според Лема 2.3 (УАТЧ-1), за всяко $x \in \mathbb{R}$ е изпълнено

$$|\rho(x)| \le \frac{1}{2}, \tag{123}$$

следователно за сумата S е налице тривиалната оценка

$$|S| \le \frac{1}{2}q.$$

Оттук виждаме, че (117) е вярно при $q \le 4h+6$ и тогава можем да считаме, че

$$q > 4h + 6. \tag{124}$$

Разделяме сумата S, зададена чрез (121) на две части

$$S = S_1 + S_2, \tag{125}$$

където

$$S_1 = \sum_{k=0}^{H} \rho\left(\frac{k+\xi_2(k)}{q}\right), \qquad S_2 = \sum_{k=H+1}^{q-1} \rho\left(\frac{k+\xi_2(k)}{q}\right) \tag{126}$$

и където

$$H = q - [h+\eta] - 1. \tag{127}$$

От (126) и (127) се вижда, че сумата S_2 притежава не повече от $h+2$ събираеми, следователно, като вземем предвид (123), получаваме

$$|S_2| \le \frac{h}{2} + 1. \tag{128}$$

За да оценим S_1, забелязваме, че от (118), (122) и (127) следва, че при $0 \le k \le H$ имаме

$$0 \le \frac{\eta}{q} \le \frac{k+\eta_2(k)}{q} \le \frac{k+\eta+h}{q} \le \frac{q-[h+\eta]-1+\eta+h}{q} < 1$$

и тогава

$$\rho\left(\frac{k+\eta_2(k)}{q}\right) = \frac{1}{2} - \left\{\frac{k+\xi_2(k)}{q}\right\} = \frac{1}{2} - \frac{k+\xi_2(k)}{q} \qquad \text{при} \qquad 0 \le k \le H.$$

Оттук и от (126) виждаме, че

$$S_1 = S_1' - S_1'', \tag{129}$$

където

$$S_1' = \sum_{k=0}^{H} \left(\frac{1}{2} - \frac{k}{q} \right), \qquad S_1'' = \frac{1}{q} \sum_{k=0}^{H} \xi_2(k). \tag{130}$$

От (118), (122), (127) и (130) очевидно следва

$$0 \leq S_1'' \leq h + 1, \tag{131}$$

а като използуваме известното тъждество $\sum_{k=1}^{m} k = \frac{m(m+1)}{2}$, намираме

$$S_1' = \frac{H+1}{2} - \frac{H(H+1)}{2q}$$

От (118), (124), (127) и от горната формула след прости изчисления, които оставяме на читателя, получаваме

$$|S_1'| \leq \frac{h}{2} + 1. \tag{132}$$

Оценката (117) следва от (125), (128), (129), (131) и (132).

□

В следващата лема оценяваме специална сума от вида (111).

Лема 4.3. *Нека $\mu, \rho \in \mathbb{R}$, $\rho > 0$, $\mu \geq 1$; $M \in \mathbb{Z}$, $q \in \mathbb{N}$, $a \in \mathbb{Z}$, като $(a, q) = 1$. Нека $f(x)$ е два пъти непрекъснато диференцируема функция в интервала $[M, M+q-1]$, която удовлетворява условията*

$$\left| f'(M) - \frac{a}{q} \right| \leq \frac{1}{q^2} \tag{133}$$

и

$$\rho \leq |f''(x)| \leq \mu\rho \qquad \textit{при} \qquad x \in [M, M+q-1]. \tag{134}$$

Тогава за сумата

$$S = \sum_{n=M}^{M+q-1} \rho(f(n)) \tag{135}$$

е в сила оценката

$$|S| \leq 7 + 2\mu\rho q^3 \tag{136}$$

Доказателство. Прилагаме формулата на Тейлор и получаваме

$$S = \sum_{n=0}^{q-1} \rho(f(M+n)) = \sum_{n=0}^{q-1} \rho\left(f(M) + f'(M)n + \frac{f''(\omega_n)}{2}n^2\right), \tag{137}$$

където $\omega_n \in [M, M+q-1]$. Като използуваме (133), записваме $f'(M)$ във вида

$$f'(M) = \frac{a}{q} + \frac{\theta}{q^2}, \qquad \text{където} \qquad \theta = \theta(M,a,q), \qquad |\theta| \le 1. \tag{138}$$

От (137) и (138) следва

$$S = \sum_{n=0}^{q-1} \rho\left(\frac{an + \xi(n)}{q}\right),$$

където

$$\xi(n) = f(M)q + \frac{\theta n}{q} + \frac{f''(\omega_n)}{2}qn^2. \tag{139}$$

Сега, като използуваме (134), (138) и (139), виждаме, че

$$|\xi(n) - f(M)q| \le \frac{n}{q} + \frac{\mu\rho}{2}qn^2 \le 1 + \frac{\mu\rho}{2}q^3 \qquad \text{при} \qquad 0 \le n \le q-1.$$

Тогава, като приложим Лема 4.2 с $h = 2 + \mu\rho q^3$, получаваме (136), с което лемата е доказана.

□

4.3 Доказателство на Теорема 4.1

Без ограничение на общността можем да считаме, че $\rho < \frac{1}{10}$, тъй като в противен случай (115) е следствие от тривиалната оценка $|T| \le \frac{1}{2}(b-a+1)$.

Съществена роля в доказателството играе лемата на Дирихле за приближаване на реални числа с рационални (Теорема 3.83. (УАТЧ-1)). Полагаме

$$\tau = \rho^{-\frac{1}{3}} \tag{140}$$

и образуваме редица от цели числа $M_1, \ldots, M_{s+1}$, удовлетворяващи

$$a < M_1 < M_2 < \cdots < M_s < M_{s+1} \le b, \tag{141}$$

по следния начин.

Полагаме $M_1 = [a] + 1$.

Ако сме определили M_i и ако е налице условието

$$b - M_i \ge \tau, \tag{142}$$

то прилагаме лемата на Дирихле и намираме $a_i \in \mathbb{Z}$, $q_i \in \mathbb{N}$ такива, че

$$\left| f'(M_i) - \frac{a_i}{q_i} \right| < \frac{1}{q_i\tau}, \qquad q_i \le \tau, \qquad (a_i, q_i) = 1, \tag{143}$$

след което определяме

$$M_{i+1} = M_i + q_i. \tag{144}$$

Тази процедура продължаваме дотогава, докато се изпълнява (142), следователно за M_{s+1} имаме

$$0 \leq b - M_{s+1} < \tau. \tag{145}$$

От (111), (141) и (144) виждаме, че

$$T = \sum_{i=1}^{s} T_i + T^*, \tag{146}$$

където

$$T_i = \sum_{n=M_i}^{M_i+q_i-1} \rho(f(n)), \qquad T^* = \sum_{n=M_{s+1}}^{[b]} \rho(f(n)). \tag{147}$$

От (123) и (145) следва, че

$$|T^*| \leq \frac{1}{2}([b] - M_{s+1} + 1) \leq \tau.$$

Тогава, вследствие на (146), имаме

$$|T| \leq \sum_{i=1}^{s} |T_i| + \tau. \tag{148}$$

От последната формула виждаме, че оценяването на сумата T се свежда до оценяване на всяка от сумите T_i, както и на числото s.

Първо ще разгледаме сумите T_i. От (143) следва, че

$$\left| f'(M_i) - \frac{a_i}{q_i} \right| < \frac{1}{q_i^2}$$

и тогава, като използуваме Лема 4.3 и също условието (140), получаваме

$$|T_i| \leq 7 + 2\mu\rho q_i^3 \ll 1 + \mu\rho\tau^3 \ll \mu.$$

От последното неравенство и от (148) следва

$$|T| \ll \mu s + \tau. \tag{149}$$

За да довършим доказателството остава да оценим отгоре величината s. За всяко естествено число $q \leq \tau$ означаваме с $m(q)$ броя на индексите i, за които $q_i = q$ и тогава очевидно имаме

$$s = \sum_{q \leq \tau} m(q). \tag{150}$$

За да оценим отгоре $m(q)$, забелязваме, че

$$m(q) = \sum_{\substack{a\in\mathbb{Z}\\(a,q)=1}} l(a,q), \tag{151}$$

където $l(a,q)$ означава броя на индексите i, за които

$$a_i = a, \qquad q_i = q. \tag{152}$$

Както ще видим по-долу, при зададено q ще имаме $l(a,q) \neq 0$ само при краен брой стойности на a, така че сумата в (151) всъщност е крайна.

Първо ще оценим $l(a,q)$ при фиксирани a и q. Нека за простота пишем $l = l(a,q)$ и нека индексите i, за които е изпълнено (152), (ако въобще такива индекси има), са числата $i_1 < i_2 < \cdots < i_l$. От (143) и (152) виждаме, че за всеки такъв индекс i_ν е изпълнено

$$\frac{a}{q} - \frac{1}{q\tau} < f'(M_{i_\nu}) < \frac{a}{q} + \frac{1}{q\tau}. \tag{153}$$

Като използуваме (144) виждаме, че

$$M_{i_{\nu+1}} - M_{i_\nu} \geq M_{i_\nu+1} - M_{i_\nu} = q_{i_\nu} = q \qquad \text{за всяко} \qquad \nu \leq l-1,$$

откъдето

$$M_{i_l} - M_{i_1} = \sum_{\nu=1}^{l-1} \left(M_{i_{\nu+1}} - M_{i_\nu}\right) \geq (l-1)q. \tag{154}$$

По-нататък, от теоремата за средните стойности следва, че за някое $\xi \in [M_{i_1}, M_{i_l}]$, е изпълнено

$$f'(M_{i_l}) - f'(M_{i_1}) = f''(\xi)(M_{i_l} - M_{i_1}).$$

Тогава, като използуваме (114) и (154), виждаме, че

$$|f'(M_{i_l}) - f'(M_{i_1})| \geq \rho(M_{i_l} - M_{i_1}) \geq \rho q(l-1).$$

От друга страна, от (153) виждаме, че

$$|f'(M_{i_l}) - f'(M_{i_1})| \leq \left|f'(M_{i_l}) - \frac{a}{q}\right| + \left|f'(M_{i_1}) - \frac{a}{q}\right| \leq \frac{2}{q\tau}.$$

От последните две формули следва $\rho q(l-1) \leq \frac{2}{q\tau}$, или все едно

$$l = l(a,q) \leq 1 + \frac{2}{\rho q^2 \tau}. \tag{155}$$

Сега за произволно $q \leq \tau$ ще оценим отгоре броя на ненулевите събираеми в сумата от дясната страна на (151). Да предположим, че a_1 и a_2 са две стойности на a, за които $l(a,q) \neq 0$, нека M_{j_1}, M_{j_2} са измежду числата $M_1, \ldots, M_s$, определени в началото на доказателството, и нека

$$\left|f'(M_{j_\nu}) - \frac{a_\nu}{q}\right| < \frac{1}{q\tau}, \qquad \nu = 1, 2. \tag{156}$$

Можем да считаме, че $a_1 \leq a_2$. От теоремата за средните стойности следва, че за някое $\eta \in [a, b]$ е изпълнено

$$f'(M_{j_2}) - f'(M_{j_1}) = f''(\eta)(M_{j_2} - M_{j_1})$$

и тогава, като използуваме (134), (141) и (156), получаваме

$$\begin{aligned}
\frac{a_2 - a_1}{q} &\leq \left| \frac{a_2}{q} - f'(M_{j_2}) \right| + |f'(M_{j_2}) - f'(M_{j_1})| + \left| f'(M_{j_1}) - \frac{a_1}{q} \right| \\
&\leq |f'(M_{j_2}) - f'(M_{j_1})| + \frac{2}{q\tau} \\
&\leq \mu\rho |M_{j_2} - M_{j_1}| + \frac{2}{q\tau} \\
&\leq \mu\rho(b-a) + \frac{2}{q\tau}.
\end{aligned}$$

Оттук следва

$$a_2 - a_1 \leq \mu\rho q(b-a) + 2.$$

И така, в сумата от (151) стойностите на a, за които $l(a, q) \neq 0$, се съдържат в интервал с дължина ненадминаваща $\mu\rho q(b-a)+2$, следователно тази сума притежава най-много $\mu\rho q(b-a)+3$ събираеми.

Тогава, като използуваме (151) и (155), виждаме, че

$$m(q) \leq \left(1 + \frac{2}{\rho q^2 \tau}\right)(\mu\rho q(b-a) + 3) \ll \mu\rho q(b-a) + \frac{\mu(b-a)}{q\tau} + \frac{1}{\rho q^2 \tau} + 1.$$

Сега прилагаме (140), (150), както и оценките от Лема 2.6 (УАТЧ-1), и получаваме

$$\begin{aligned}
s &\ll \mu\rho(b-a) \sum_{q \leq \tau} q + \frac{\mu(b-a)}{\tau} \sum_{q \leq \tau} \frac{1}{q} + \frac{1}{\rho\tau} \sum_{q \leq \tau} \frac{1}{q^2} + \tau \\
&\ll \mu\rho\tau^2(b-a) + \frac{\mu(b-a)}{\tau} \log(\tau + 1) + \frac{1}{\rho\tau} + \tau \\
&\ll \left(\mu\rho^{\frac{1}{3}}(b-a) + \rho^{-\frac{2}{3}}\right) \log\left(\rho^{-1} + 2\right).
\end{aligned}$$

Остава да вземем под внимание (140) и (149) и получаваме оценката (115), с което теоремата е доказана.

□

5 Въведение в методите на решетото

5.1 Решето на Ератостен – Льожандър

Ще започнем със следната лема, която ни дава явна формула за функцията $\pi(x)$, която изучавахме в Глава 5 (УАТЧ-1) и която означава броя на простите числа ненадминаващи x.

Лема 5.1. *За всяко реално $x \geq 2$ е в сила формулата*

$$\pi(x) = \pi(\sqrt{x}) - 1 + \sum_{d|P} \mu(d) \left[\frac{x}{d}\right], \tag{157}$$

където $\mu(d)$ е функцията на Мьобиус и

$$P = \prod_{p \leq \sqrt{x}} p. \tag{158}$$

Доказателство. Да означим с S броя на естествените числа $n \leq x$, които са взаимно прости с P. Като използваме основното свойство на функцията на Мьобиус, дадено в Лема 3.34 (УАТЧ-1), виждаме, че

$$S = \sum_{n \leq x} \sum_{d|(n,P)} \mu(d).$$

Сменяме реда на сумиране и прилагаме Определение 3.3 (УАТЧ-1). Получаваме

$$S = \sum_{d|P} \mu(d) \sum_{\substack{n \leq x \\ d|n}} 1 = \sum_{d|P} \mu(d) \left[\frac{x}{d}\right]. \tag{159}$$

От друга страна, като използуваме (158), виждаме, че едно естествено число $n \leq x$ е взаимно просто с P точно когато n е просто число, лежащо в интервала $(\sqrt{x}, x]$, или пък ако $n = 1$. Наистина, случаят $n = 1$ е тривиален. По-нататък, ако $1 < n \leq \sqrt{x}$, то очевидно $(n, P) > 1$. Да разгледаме накрая случая $\sqrt{x} < n \leq x$. Тогава, ако n е просто, то $(n, P) = 1$, а ако n е съставно, то притежава прост делител, ненадминаващ $\sqrt{x}$ (виж Лема 3.8 (УАТЧ-1)), следователно $(n, P) > 1$. От горните разсъждения следва, че

$$S = \pi(x) - \pi(\sqrt{x}) + 1. \tag{160}$$

От (159) и (160) получаваме (157), с което лемата е доказана.

□

При малки стойности на x е възможно използуването на тъждеството от Лема 5.1 за получаване на информация за порядъка на $\pi(x)$. Ако обаче x е голямо възникват непреодолими трудности, основната причина за които е фактът, че величината P, определена чрез (158), има твърде много делители, вследствие на което сумата в

дясната страна на (157) има много голям брой събираеми. Въпреки това ще разсъждаваме още малко върху формулата (157). От нея веднага следва, че

$$\pi(x) = \sum_{d|P} \mu(s) \left(\frac{x}{d} - \left\{ \frac{x}{d} \right\} \right) + O\left(\sqrt{x}\right)$$

$$= x \sum_{d|P} \frac{\mu(d)}{d} - \sum_{d|P} \mu(d) \left\{ \frac{x}{d} \right\} + O\left(\sqrt{x}\right) \tag{161}$$

Като използуваме (158), Лема 3.38, Лема 3.40 и Лема 5.12 (заедно със забележката след нея) от (УАТЧ-1), виждаме, че

$$\sum_{d|P} \frac{\mu(d)}{d} = \prod_{p \leq \sqrt{x}} \left(1 - \frac{1}{p}\right) = \frac{e^{-\gamma}}{\log \sqrt{x}} \left(1 + O\left(\frac{1}{\log x}\right)\right). \tag{162}$$

По-нататък, от (158), от Определение 3.17 (УАТЧ-1), както и от Лема 3.32 (УАТЧ-1) следва

$$\left| \sum_{d|P} \mu(d) \left\{ \frac{x}{d} \right\} \right| \leq \tau(P) = 2^{\pi(\sqrt{x})}. \tag{163}$$

Като вземем предвид (161) – (163) получаваме

$$\pi(x) = 2e^{-\gamma} \frac{x}{\log x} + O\left(\frac{x}{\log^2 x}\right) + O\left(2^{\pi(\sqrt{x})}\right). \tag{164}$$

Последната формула, обаче, е безполезна. Наистина, според теоремата на Чебишев (Теорема 5.4 (УАТЧ-1)) имаме $\pi(x) \gg \frac{x}{\log x}$ и оттук следва, че функцията $2^{\pi(\sqrt{x})}$ нараства по-бързо от коя да е степен на x и, в частност, по порядък значително надвишава първото събираемо в дясната страна на (164).

Да отбележим също, че според асимптотичния закон за разпределение на простите числа (Теорема 5.34 (УАТЧ-1)) имаме $\pi(x) \sim \frac{x}{\log x}$ при $x \to \infty$. Тъй като $2e^{-\gamma} \neq 1$, първото събираемо в дясната страна на равенство (164) няма как да бъде правилното приближение за $\pi(x)$, или с други думи, една част от главния член в асимптотичната формула за $\pi(x)$ е „скрита" в сумата $\sum_{d|P} \mu(d) \left\{ \frac{x}{d} \right\}$.

Въпреки това идеята от горните разсъждения е ползотворна и чрез подходяща модификация и усъвършенстване на изложения метод могат да се получат интересни резултати. Льожандър чрез подобни пресмятания е намерил първата нетривиална оценка отгоре за $\pi(x)$ при достатъчно големи x, а именно

$$\pi(x) \ll \frac{x}{\log \log x}. \tag{165}$$

Тази оценка е по-слаба от оценката на Чебишев за $\pi(x)$ (виж Теорема 5.4 (УАТЧ-1)), но е получена по-рано. Освен това, по същия начин може да се установи следната теорема, която е обобщение на (165), но вече не може да се получи като следствие от теоремата на Чебишев.

Теорема 5.2 (Льожандър)**.** *Ако* $10 < h \leq x$*, то е в сила неравенството*

$$\pi(x) - \pi(x-h) \ll \frac{h}{\log\log h}, \tag{166}$$

като константата в знака $\ll$ *е абсолютна.*

С други думи, ако вземем дори и много къс интервал от вида $(x-h, x]$, то почти всички цели числа в него са съставни.

Доказателство. Нека z е параметър, който ще изберем по-късно. Полагаме

$$P = \prod_{p \leq z} p. \tag{167}$$

Ако едно цяло число $n > z$ е просто, то очевидно е изпълнено $(n, P) = 1$. Тогава

$$\pi(x) - \pi(x-h) \leq z + S, \tag{168}$$

където $S = S(x, h, z)$ е броя на числата $n \in (x-h, x]$, за които $(n, P) = 1$.

За да оценим S прилагаме Лема 3.34 (УАТЧ-1), след което сменяме реда на сумиране. Получаваме

$$S = \sum_{x-h<n\leq x} \sum_{d|(n,P)} \mu(d) = \sum_{d|P} \mu(d)\, \Gamma(x, h, d), \tag{169}$$

където $\Gamma(x, h, d)$ е броя целите числа от интервала $(x-h, x]$, които се делят на d. Очевидно имаме

$$\Gamma(x, h, d) = \left[\frac{x}{d}\right] - \left[\frac{x-h}{d}\right] = \frac{h}{d} + O(1)$$

и, като заместим в (169), намираме

$$S = h \sum_{d|P} \frac{\mu(d)}{d} + O(\tau(P)). \tag{170}$$

Сега, като разсъждаваме както при доказателството на формула (162), получаваме

$$\sum_{d|P} \frac{\mu(d)}{d} \ll (\log z)^{-1}, \tag{171}$$

а като приложим Лема 3.32 (УАТЧ-1) виждаме, че

$$\tau(P) = 2^{\pi(z)} \leq 2^z. \tag{172}$$

От (168) и (170) – (172) следва

$$\pi(x) - \pi(x-h) \ll \frac{h}{\log z} + 2^z.$$

Остава да положим $z = \log h$ и получаваме (166).

□

Да отбележим, че резултатът на Теорема 5.2 може да бъде значително усилен. Като се използуват по-сложни методи, с които ще се запознаем в следващите параграфи, може да бъде доказана следната

Теорема 5.3. *Ако* $10 < h \leq x$, *то*

$$\pi(x) - \pi(x-h) \ll \frac{h}{\log h}, \tag{173}$$

като константата в знака $\ll$ *е абсолютна.*

□

Оценяването на константата на Виноградов от формула (173) също представлява интерес и, както е установено от Монтгомери и Вон, тя може да бъде взета равна на 2. Получени са аналогични резултати и за броя на простите числа в къс интервал и принадлежащи на дадена аритметична прогресия. В настоящите записки няма да привеждаме доказателства на Теорема 5.3 и на нейни обобщения. Читателят би могъл да намери такива в монографиите [12] и [13].

5.2 Някои резултати, получени чрез методите на решетото

Както видяхме в параграф 5.1, с помощта решетото на Ератостен–Льожандър могат да бъдат получени не много силни, но все пак нетривиални резултати. Първото съществено подобрение на това решето е направено от Брун през двадесетте години на миналия век. В настоящата глава ще приложим най-простия вариант на решетото на Брун, за да докажем теорема, отнасяща се до така наречените *прости числа близнаци.*

Ще поясним какво означава последният термин. Ако разгледаме таблицата на първите прости числа ще забележим, че твърде често се появяват двойки прости числа, които се различават с 2. Такива са например двойките 3 и 5, 11 и 13, 17 и 19, 41 и 43, както и още много други. Най-големите прости числа от такъв вид, известни до този момент, са

$$65516468355 \cdot 2^{333333} \pm 1,$$

като всяко от тях притежава 100355 цифри в десетичното си представяне. [2]

Определение 5.4. *Всеки две прости числа, които имат разлика* 2, *се наричат прости числа близнаци.*

Още в древността е възникнала следната

Хипотеза 5.5. *Съществуват безбройно много двойки от прости числа близнаци.*

[2] По-подробна информация може да се намери на следната интернет страница:

http://primes.utm.edu/primes/page.php?id=89650

Тази хипотеза и в настоящия момент не е доказана и се счита, че е един от най-трудните нерешени проблеми в теорията на числата.

За изучаването на простите числа близнаци е удачно въвеждането на следното

Определение 5.6. *Означаваме с $\pi^*(x)$ броя на простите числа $p \leq x$, за които $p+2$ също е просто число.*

При това означение Хипотеза 5.5 е еквивалентна на равенството

$$\lim_{x\to\infty} \pi^*(x) = \infty, \tag{174}$$

което, както вече изяснихме, не е доказано.

И така, нетривиална оценка отдолу за $\pi^*(x)$, от която да следва (174) в настоящия момент не е известна. Получени са обаче нетривиални оценки отгоре за тази величина, като тези оценки са твърде близки до предполагаемата стойност на $\pi^*(x)$.

За да направим преположение относно порядъка на $\pi^*(x)$ ще изложим някои популярни (и математически нестроги) разсъждения. Според теоремата на Чебишев, и също според асимптотичния закон за разпределение на простите числа, разгледани в Глава 5 (УАТЧ-1), при големи стойности на x величината $\pi(x)$ е приблизително равна на $\frac{x}{\log x}$. Това твърдение би могло да се тълкува по следния начин:

Ако вземем случайно число ненадминаващо x, вероятността то да е просто е приблизително равна на $\frac{1}{\log x}$.

Разбира се, от математическа гледна точка, горното твърдение е некоректно, но въпреки това ще продължим да разсъждаваме по този (наивен) начин.

Нека имаме двойка естествени числа $n, n+2$ ненадминаващи x. Тъй като вероятността n да е просто е $\frac{1}{\log x}$, а вероятността $n+2$ да е просто е също толкова, то вероятността и двете числа $n, n+2$ да са прости е $\frac{1}{\log^2 x}$, следователно има приблизително $\frac{x}{\log^2 x}$ прости числа $n \leq x$, за които $n+2$ също е просто. С други думи, би трябвало да е изпълнено $\pi^*(x) \asymp \frac{x}{\log^2 x}$.

Разсъжденията от горния тип нямат математическа стойност по ред причини. Достатъчно е да споменем само, че ако числото n е четно, то и $n+2$ е четно, така че „събитията" „n е просто" и „$n+2$ е просто" няма как да са независими. С помощта на по-прецизни, но също толкова математически необосновани разсъждения, може да се изкаже следната хипотеза, която представлява значително усилване на Хипотеза 5.5.

Хипотеза 5.7. *В сила е асимптотичната формула*

$$\pi^*(x) \sim c_0 \frac{x}{\log^2 x} \qquad \textit{при} \qquad x \to \infty, \tag{175}$$

където

$$c_0 = 2\prod_{p>2}\left(1 - \frac{1}{(p-1)^2}\right) = 1.3203236\ldots. \tag{176}$$

Константата c_0, определена по-горе, е известна като *константа на Брун*.

Интересно е, че Хипотеза 5.7 може да бъде обоснована и като се използува така наречения *кръгов метод* на Харди и Литлууд, разработен от тези учени през двадесетте години на миналия век. По-точно, чрез формално прилагане на кръговия метод може да бъде получена формула за $\pi^*(x)$, в която тази величина е представена като сума на няколко събираеми. Едно от тях е изразът от дясната страна на (175) и се предполага, че той е главният член. Има основания да се очаква, че останалите събираеми са „малки", но въпреки усилията на много математици през последните 90 години, това все още не е доказано.

Значителен (макар и частичен) успех при изучаването на $\pi^*(x)$ е намирането на точна по порядък оценка отгоре (т.е. оценка, съгласувана с Хипотеза 5.7). В сила е следната

Теорема 5.8. *При $x \geq 2$ е изпълнено*

$$\pi^*(x) \ll \frac{x}{\log^2 x}. \tag{177}$$

Този резултат е получен от Брун, а по-късно алтернативни доказателства са намерени от Селберг и от други математици. Ще отбележим, че установяването на формула (177) с колкото се може по-малка константа в знака на Виноградов също е интересна и трудна задача. В настоящия момент е известно, че ако x е достатъчно голямо, тази константа може да се вземе равна на $3.5\, c_0$, където c_0 е константата на Брун, определена чрез (176).

Доказателство на Теорема 5.8 няма да привеждаме, но в настоящата глава ще разгледаме решетото на Селберг и ще го приложим за оценяване отгоре величина подобна на $\pi^*(x)$. След малки промени в разсъжденията ще можем да получим също и доказателство на оценката (177).

В следващия параграф ще формулираме и докажем Теорема 5.12, която представлява малко по-слаб вариант на Теорема 5.8, но все пак е достатъчно интересна. При това, доказателството, което ще изложим, е сравнително просто и ще даде на читателя представа за техниката, която се използува в методите на решетото.

Накрая съвсем накратко ще се спрем на нерешената задача за намиране на нетривиална оценка отдолу на $\pi^*(x)$ и на някои теореми, свързани с нея. Ясно е, че ако е вярна Хипотеза 5.7, то ще е изпълнено $\pi^*(x) \gg \frac{x}{\log^2 x}$. Брун е доказал теорема, която, в известен смисъл, е приближение към горната оценка.

За да формулираме резултата на Брун, ще въведем някои означения. Нека за произволно $r \in \mathbb{N}$ означим с $\mathcal{P}_r$ множеството от естествени числа, притежаващи в каноничното си разлагане не повече от r на брой прости множителя (всеки броен толкова пъти, колкото е кратността му). [3] Числата от $\mathcal{P}_r$ се наричат *почти прости*

[3] Например, $\mathcal{P}_1$ е множеството от простите числа, а $\mathcal{P}_2$ е множеството от числата, които са прости, или са квадрат на просто число, или са произведение на две различни прости числа.

от ред r. По-нататък, за произволни $r, l \in \mathbb{N}$ определяме

$$\Pi_{r,l}(x) = \#\left\{n \in \mathbb{N} \,:\, n \leq x,\ n \in \mathcal{P}_r,\ n+2 \in \mathcal{P}_l\right\}.$$

(При това означение имаме $\Pi_{1,1}(x) = \pi^*(x)$.)

Използувайки усъвършенстван вариант на своето решето, Брун е доказал следната теорема, чието доказателство няма да излагаме

Теорема 5.9 (Брун, 1917)**.** *При* $x \geq 2$ *е изпълнено*

$$\Pi_{7,7}(x) \gg \frac{x}{\log^2 x}.$$

□

Тази теорема е подобрявана многократно и най-силният резултат от този тип е следната знаменита

Теорема 5.10 (Чен, 1973)**.** *При* $x \geq 2$ *е изпълнено*

$$\Pi_{1,2}(x) \gg \frac{x}{\log^2 x}.$$

□

От Теорема 5.10 следва, в частност, че съществуват безбройно много прости числа p такива, че $p+2$ притежава в каноничното си разлагене най-много два прости множителя. Теоремата на Чен е едно от най-значимите постижения в аналитичната теория през 20-ти век. Интересуващият се читател може да намери нейното доказателство в някоя от монографиите [12] и [13].

Накрая ще формулираме един изключително интересен и важен резултат, получен съвсем наскоро. Нека p_n означава n-тото просто число. Тогава Хипотеза 5.5 е еквивалентна на твърдението, че съществуват безбройно много n, за които

$$p_{n+1} - p_n = 2.$$

През последните години Голдстон, Пинц и Ялдарим (виж [10], [11]) установиха, че за безбройно много n разликата $p_{n+1} - p_n$ е „малка" (по-подробна информация може да се намери в горепосочените статии). През май 2013 г. У. Джанг [23] подобри значително резултатите на Голдстон, Пинц и Ялдарим и доказа че има безбройно много двойки от прости числа, които са на разстояние по-малко от фиксирана константа. По-точно, в сила е следната

Теорема 5.11 (Джанг, 2013)**.** *Съществуват безбройно много* n *такива, че*

$$p_{n+1} - p_n < 7 \cdot 10^7.$$

Появата на този резултат беше изненада за специалистите по теория на числата, тъй като се считаше, че получаването му е извън възможностите на съвременната математика. След публикуването на статията на Джанг със задачата за подобряване на константата $7 \cdot 10^7$ се заеха редица математици и към настоящия момент[4] най-силният резултат в това направление принадлежи на Пинц [20], като в неговата версия на Теорема 5.11 константата е равна на 2 530 338.

Теоремата на Джанг е едно от най-значимите постижения на съвременната теория на числата. Можем да се надяваме, че няма да е далече денят, в който ще бъде доказана и хипотезата за простите числа близнаци.

5.3 Най-простото решето на Брун

5.3.1 Формулировка на теоремата и нейно следствие

В настоящия параграф ще формулираме и докажем следната теорема, която представлява леко отслабен вариант на Теорема 5.8.

Теорема 5.12 (Брун)**.** *При $x \geq 10$ е изпълнено*

$$\pi^*(x) \ll \frac{x\,(\log\log x)^2}{(\log x)^2}. \tag{178}$$

Да отбележим, че от теоремата на Мертенс (Лема 5.11 (УАТЧ-1)) следва, че редът, съставен от реципрочните стойности на всички прости числа е разходящ. От друга страна, от Теорема 5.12 получаваме

Следствие 5.13. *Редът, съставен от реципрочните стойности на простите числа, участващи в някоя от двойките прости близнаци, е сходящ.*

Доказателство. Достатъчно е да докажем, че е сходящ редът, съставен от реципрочните стойности на първите числа от всяка двойка прости близнаци. За тази цел ще докажем, че частичните суми на този ред

$$S(x) = \sum_{\substack{p \leq x \\ p+2 \text{ — просто}}} \frac{1}{p} \tag{179}$$

са ограничени. Използуваме преобразованието на Абел (Лема 2.1 (УАТЧ-1)), Определение 5.6, Теорема 5.12, както и елементарните свойства на несобствените интеграли, и виждаме, че при $x \geq 10$ е изпълнено

$$S(x) = \frac{\pi^*(x)}{x} + \int\limits_2^x \frac{\pi^*(t)}{t^2}\,dt \ll 1 + \int\limits_{10}^x \frac{(\log\log t)^2}{t(\log t)^2}\,dt \ll 1.$$

С това следствието е доказано.

□

[4] 11 юни 2013 г.

5.3.2 Идея на доказателството и помощни леми

Можем да считаме, че x е достатъчно голямо и нека z е параметър, който в края на доказателството ще изберем в зависимост от x. Засега считаме само, че z е достатъчно голямо и че

$$z < \sqrt{x}. \tag{180}$$

Полагаме

$$D = \prod_{p \le z} p. \tag{181}$$

Нека S_0 означава броя на простите числа $p \in (z, x]$, за които числото $p+2$ също е просто. Тогава от определението на $\pi^*(t)$ очевидно следва, че

$$S_0 = \pi^*(x) - \pi^*(z).$$

По-нататък, от (181) се вижда, че за всяко от простите числа p, преброени в S_0, числата $p(p+2)$ и D са взаимно прости. Следователно, ако S_1 е броя на естествените числа $n \le x$, за които $n(n+2)$ е взаимно просто с D, то имаме

$$\pi^*(x) \le S_0 + z \le S_1 + z. \tag{182}$$

От последното неравенство се вижда, че за да докажем теоремата трябва да изберем по подходящ начин параметъра z и да намерим достатъчно добра оценка отгоре за величината S_1. Да отбележим, че вследствие на Лема 3.34 (УАТЧ-1) тя може се запише във вида

$$S_1 = \sum_{n \le x} \sum_{d \mid (n(n+2), D)} \mu(d). \tag{183}$$

Нека се опитаме първо да приложим решетото на Ератостен–Льожандър, което разгледахме в параграф 5.1. Този опит ще е безуспешен, но ще ни помогне да разберем как трябва да се модифицира метода, за да получим нетривиален резултат.

Ако сменим реда на сумиране в израза от дясната страна на (183) ще получим

$$S_1 = \sum_{d \mid D} \mu(d)\, T(x, d), \tag{184}$$

където

$$T(x, d) = \#\{n \in \mathbb{N} \,:\, n \le x, \quad n(n+2) \equiv 0 \pmod{d}\}. \tag{185}$$

От Лема 3.56 (УАТЧ-1) следва

$$T(x, d) = x\frac{\beta(d)}{d} + O(\beta(d)), \tag{186}$$

като константата в знака O е абсолютна, а $\beta(d)$ е мултипликативна функция на d, която се определя чрез

$$\beta(d) = \#\{\, n \in \mathbb{N} \,:\, 1 \le n \le d, \;\; n(n+2) \equiv 0 \pmod{d} \,\}. \tag{187}$$

Сега, ако заместим последния израз за $T(x,d)$ в (184), ще получим

$$S_1 = xS_1' + O\left(S_1''\right), \tag{188}$$

където

$$S_1' = \sum_{d|D} \mu(d)\,\frac{\beta(d)}{d}, \qquad S_1'' = \sum_{d|D} \beta(d). \tag{189}$$

За да изследваме сумата S_1' ще използуваме следната лема, която е обобщение на една от формулите на Мертенс (Лема 5.12 (УАТЧ-1)). Доказателството ѝ не се различава съществено от доказателството на тази формула на Мертенс, поради което го оставяме на читателя.

Лема 5.14. *Ако е дадено произволно $a \in \mathbb{R}$, то при $x > \max(2,-a)$ е в сила асимптотичната формула*

$$\prod_{-a<p\le x} \left(1+\frac{a}{p}\right) = c(a)(\log x)^a + O\left((\log x)^{a-1}\right),$$

където $c(a) \in \mathbb{R}$, $c(a) > 0$ и константата в знака O зависи от a.

□

От Лема 3.56 (УАТЧ-1) знаем, че функцията $\beta(d)$, определена чрез (187), е мултипликативна. Виждаме също, че ако p е просто число, то

$$\beta(p) = \begin{cases} 1 & \text{ако } p = 2, \\ 2 & \text{ако } p > 2. \end{cases} \tag{190}$$

Тогава от (181), (189) и Лема 5.14 следва

$$S_1' = \prod_{p|D}\left(1-\frac{\beta(p)}{p}\right) = \frac{1}{2}\prod_{2<p\le z}\left(1-\frac{2}{p}\right) = \frac{c}{\log^2 z}\left(1+O\left(\frac{1}{\log z}\right)\right),$$

където $c > 0$ е константа. Оттук получаваме

$$S_1' \ll \frac{1}{\log^2 z}. \tag{191}$$

Сега се налага да оценим и сумата S_1'', определена чрез (189), след което трябва да използуваме (188) и (191) и накрая да изберем по подходящ начин параметъра z и така да оценим S_1. При реализацията на този план обаче възникват непреодолими трудности. Наистина, от (190) виждаме, че $1 \le \beta(d) \le 2$, следователно

$$2^{\pi(z)} = \tau(D) \le S_1'' \le \tau^2(D) = 4^{\pi(z)}. \tag{192}$$

Ако използуваме (182), (188), (191) и (192) и ако след това изберем z по оптимален начин, ще получим

$$\pi^*(x) \ll \frac{x}{(\log\log x)^2}.$$

Тази оценка, обаче, е по-слаба дори от тривиалната оценка

$$\pi^*(x) \leq \pi(x) \ll \frac{x}{\log x}.$$

Следователно, ако работим по описания метод, няма как да получим доказателство на неравенство (178) от Теорема 5.12 и основната причина за това е, че сумата S_1'' притежава прекалено много събираеми.

Основната идея при съвременните методи на решетото е следната. Вместо да работим директно със сумата S_1, определена чрез (183), първо я модифицираме, като заменим сумата по d в дясната страна това равенство с подобна сума. При това искаме вече променената сума S_1' да се представя отново във вида (188), като главният член да се оценява както преди, а, което е най-важното, остатъчният член да представлява сума с не чак толкова много събираеми, поради което и за нея да може да се намери приемлива оценка.

При най-простия вариант на решетото на Брун основна роля играе следната

Лема 5.15. *Нека $\omega(n)$ означава броя на различните прости делители на естественото число n. Тогава за произволно $h \in \mathbb{N}$ са в сила неравенствата*

$$\sum_{\substack{d|n \\ \omega(d)\leq 2h-1}} \mu(d) \leq \sum_{d|n} \mu(d) \leq \sum_{\substack{d|n \\ \omega(d)\leq 2h}} \mu(d). \tag{193}$$

Да отбележим, че за доказателството на Теорема 5.12 ще имаме нужда само от дясното от неравенствата (193), но за пълнота привеждаме и лявото.

Доказателство. При $n = 1$ твърдението е очевидно и оттук нататък ще разглеждаме случая $n > 1$. Без ограничение на общността можем да считаме, че n е безквадратно и нека каноничното му разлагане на прости множители е

$$n = p_1 p_2 \dots p_s, \qquad \text{където} \qquad p_1 < p_2 < \dots < p_s.$$

За произволно $m \in \mathbb{N}$ разглеждаме сумата

$$H(n,m) = \sum_{\substack{d|n \\ \omega(d)\leq m}} \mu(d). \tag{194}$$

Като вземем предвид Лема 3.34 (УАТЧ-1), виждаме, че е достатъчно да установим неравенството

$$(-1)^m H(n,m) \geq 0. \tag{195}$$

Можем да считаме, че $m < s$, тъй като в противен случай имаме $H(n,m) = 0$ и (195) е изпълнено.

Като използваме Определение 3.19 (УАТЧ-1), както и прости комбинаторни съображения, виждаме, че

$$H(n,m) = \sum_{\substack{\nu_1,\ldots,\nu_s\in\{0,1\}\\ \nu_1+\cdots+\nu_s\le m}} \mu\left(p_1^{\nu_1}\ldots p_s^{\nu_s}\right) = \sum_{k=0}^{m} \sum_{\substack{\nu_1,\ldots,\nu_s\in\{0,1\}\\ \nu_1+\cdots+\nu_s=k}} (-1)^k$$

$$= \sum_{k=0}^{m}(-1)^k \sum_{\substack{\nu_1,\ldots,\nu_s\in\{0,1\}\\ \nu_1+\cdots+\nu_s=k}} 1 = \sum_{k=0}^{m}(-1)^k\binom{s}{k}$$

$$= 1 - \binom{s}{1} + \binom{s}{2} - \binom{s}{3} + \cdots + (-1)^m\binom{s}{m}. \tag{196}$$

Да разгледаме първо случая $m \le \frac{1}{2}s$. Тогава имаме

$$1 \le \binom{s}{1} \le \binom{s}{2} \le \cdots \le \binom{s}{m}$$

и, като вземем предвид (196), получаваме, че (195) е изпълнено.

Сега да допуснем, че

$$\frac{1}{2}s < m < s. \tag{197}$$

От (196) следва

$$H(n,m) = \sum_{k=0}^{s}(-1)^k\binom{s}{k} - \sum_{k=m+1}^{s}(-1)^k\binom{s}{k} = -\sum_{k=m+1}^{s}(-1)^k\binom{s}{k}$$

$$= -\sum_{l=0}^{s-m-1}(-1)^{s-l}\binom{s}{s-l} = (-1)^{s-1}\sum_{l=0}^{s-m-1}(-1)^l\binom{s}{l}$$

$$= (-1)^{s-1}H(n,s-m-1).$$

От (197) следва $s-m-1 \le \frac{1}{2}s$, следователно получаваме

$$(-1)^m H(n,m) = (-1)^{s-m-1}H(n,s-m-1) \ge 0,$$

с което лемата е доказана.

□

5.3.3 Доказателство на Теорема 5.12.

Като вземем предвид неравенството (182) виждаме, че за да докажем (178) е достатъчно да оценим отгоре по съответен начин сумата S_1, зададена чрез (183). Нека $k \in \mathbb{N}$ е параметър, който впоследствие ще изберем в зависимост от x. Като използуваме Лема 5.15 виждаме, че

$$S_1 \leq S_2, \tag{198}$$

където

$$S_2 = \sum_{n \leq x} \sum_{\substack{d \mid (n(n+2), D) \\ \omega(d) \leq 2k}} \mu(d). \tag{199}$$

Предстои ни да оценяваме отгоре S_2. Сменяме реда на сумиране и получаваме

$$S_2 = \sum_{\substack{d \mid D \\ \omega(d) \leq 2k}} \mu(d)\, T(x, d), \tag{200}$$

където $T(x, d)$ се определя от (185). Сега прилагаме формула (186) и намираме, че

$$S_2 = xS_2' + O(S_2''), \tag{201}$$

където

$$S_2' = \sum_{\substack{d \mid D \\ \omega(d) \leq 2k}} \frac{\mu(d)\beta(d)}{d}, \qquad S_2'' = \sum_{\substack{d \mid D \\ \omega(d) \leq 2k}} \beta(d). \tag{202}$$

Да отбележим, че равенството (201) е аналогично на (188), като сумите S_2' и S_2'' съответстват съответно на S_1' и S_1'', зададени чрез (189). При това, ограничението $\omega(d) \leq 2k$, наложено в областта на сумиране на S_2'' значително намалява броя на събираемите в тази сума, особено ако числото k не е голямо. Ако пък k не е прекалено малко, то, както ще се убедим по-долу, сумата S_2' не се отличава твърде много от S_1' и, в частност, се оценява по подобен начин. Следователно можем да очакваме, че ако изберем по оптимален начин k, а след това и z, ще можем да реализираме на практика плана, който предложихме в предишния параграф.

Първо ще изследваме сумата S_2'. Представяме я във вида

$$S_2' = S_1' - S_2^*, \tag{203}$$

където S_1' се определя чрез (189) и

$$S_2^* = \sum_{\substack{d \mid D \\ \omega(d) > 2k}} \frac{\mu(d)\beta(d)}{d}. \tag{204}$$

Вече разбрахме как се оценява S_1' и получихме неравенството (191).

Сега да разгледаме сумата S_2^*. Разделяме я на части съобразно броя на простите множители на сумационната променлива d. По-точно, нека s е броят на простите числа, ненадминаващи z, или все едно

$$s = \pi(z). \tag{205}$$

Тогава от (181) следва, че ако $d \mid D$, то d притежава най-много s на брой прости множители. Следователно можем да запишем

$$S_2^* = \sum_{l=2k+1}^{s} \sum_{\substack{d \mid D \\ \omega(d)=l}} \frac{\mu(d)\beta(d)}{d},$$

откъдето

$$|S_2^*| \leq \sum_{l=2k+1}^{s} \sum_{\substack{d \mid D \\ \omega(d)=l}} \frac{\beta(d)}{d}. \tag{206}$$

От мултипликативността на функцията $\beta(d)$ и от определението (181) за D следва, че

$$\sum_{\substack{d \mid D \\ \omega(d)=l}} \frac{\beta(d)}{d} \leq \frac{1}{l!} \left(\sum_{p \leq z} \frac{\beta(p)}{p} \right)^l. \tag{207}$$

Наистина, ако $d \mid D$ и $\omega(d) = l$, то $d = p_1 \dots p_l$, където p_j са две по две различни прости числа, ненадминаващи z. При повдигане на сумата $\sum_{p \leq z} \frac{\beta(p)}{p}$ в l-та степен събираемото

$$\frac{\beta(p_1)}{p_1} \cdots \frac{\beta(p_l)}{p_l} = \frac{\beta(d)}{d}$$

се появява $l!$ пъти. Следователно изразът от дясната страна на (207) съдържа всички събираеми на сумата от лявата страна на това неравенство, както и други неотрицателни събираеми.

По-нататък, като използуваме (190) и Лема 5.11 (УАТЧ-1) виждаме, че ако z е достатъчно голямо, то

$$\sum_{p \leq z} \frac{\beta(p)}{p} = \frac{1}{2} + 2 \sum_{2 < p \leq z} \frac{1}{p} = 2 \log\log z + O(1) \leq 3 \log\log z, \tag{208}$$

От (206) – (208) следва, че

$$|S_2^*| \leq \sum_{l=2k+1}^{s} \frac{(3 \log\log z)^l}{l!}. \tag{209}$$

Сега ще използуваме, че ако e означава неперовото число, то

$$n! > \left(\frac{n}{e}\right)^n \qquad \text{за всяко} \qquad n \in \mathbb{N}. \tag{210}$$

Това неравенство се получава като сравним величината $\log n! = \sum_{1<k\leq n} \log k$ и интеграла $\int_1^n \log t\, dt$. Елементарната проверка предоставяме на читателя.

От (209) и (210) следва

$$|S_2^*| \leq \sum_{l=2k+1}^{s} \left(\frac{10 \log\log z}{l}\right)^l \tag{211}$$

До този момент нямаше наложени ограничения върху параметъра k, но оттук нататък ще предполагаме, че

$$10 \log\log z < k. \tag{212}$$

Тогава от (211) (212) получаваме

$$|S_2^*| \leq \sum_{l=2k+1}^{\infty} \frac{1}{2^l} = \frac{1}{2^{2k}} < 2^{-20 \log\log z} = (\log z)^{-20 \log 2} < (\log z)^{-10}. \tag{213}$$

Като използуваме (191), (203) и (213) виждаме, че

$$S_2' \ll (\log z)^{-2}. \tag{214}$$

Сега ще оценим сумата S_2'', определена чрез (202). Като използуваме (181) и (190) получаваме

$$S_2'' = \sum_{l=0}^{2k} \sum_{\substack{d|D \\ \omega(d)=l}} \beta(d) \leq \sum_{l=0}^{2k} \sum_{\substack{d|D \\ \omega(d)=l}} 2^l = \sum_{l=0}^{2k} 2^l \sum_{\substack{d|D \\ \omega(d)=l}} 1.$$

По-нататък, от определението на функцията $\omega(d)$ и от (205) се вижда, че

$$\sum_{\substack{d|D \\ \omega(d)=l}} 1 = \sum_{\substack{\alpha_1,\ldots,\alpha_s\in\{0,1\} \\ \alpha_1+\cdots+\alpha_s=l}} 1 = \binom{s}{l} \leq \frac{s^l}{l!}.$$

От горните формули и от (205) получаваме

$$S_2'' \leq s^{2k} \sum_{l=0}^{2k} \frac{2^l}{l!} \leq s^{2k} \sum_{l=0}^{\infty} \frac{2^l}{l!} = e^2 s^{2k} \ll z^{2k}. \tag{215}$$

Вече сме в състояние да оценим сумата S_2, определена чрез (199). От (201), (214) и (215) следва

$$S_2 \ll \frac{x}{\log^2 z} + z^{2k}.$$

Сега, като използуваме също (182) и (198), получаваме

$$\pi^*(x) \ll \frac{x}{\log^2 z} + z^{2k}, \tag{216}$$

като константата в знака $\ll$ е абсолютна, а параметърът k удовлетворява (212).

Остава да определим параметрите k и z като функции на x по оптимален начин. За k предполагаме, че

$$k < 20 \log\log z \tag{217}$$

(Очевидно съществува $k \in \mathbb{N}$, удовлетворяващо едновременно (212) и (217)). Тогава, ако е налице условието (180), ще имаме

$$z^{2k} \leq z^{40 \log\log z} \leq z^{40 \log\log x} = e^{40\,(\log\log x)\log z}. \tag{218}$$

Определяме

$$z = \exp\left(\frac{\log x}{80 \log\log x}\right), \qquad \text{или все едно} \qquad \log z = \frac{\log x}{80 \log\log x}. \tag{219}$$

Тогава от (218) следва

$$z^{2k} \leq e^{\frac{1}{2}\log x} = \sqrt{x} \tag{220}$$

и, в частност, изпълнено е (180).

От (216), (219) и (220) получаваме

$$\pi^*(x) \ll \frac{x\,(\log\log x)^2}{(\log x)^2},$$

с което теоремата е доказана.

□

5.4 Решето на Селберг и приложение към бинарния проблем на Голдбах

5.4.1 Формулировка на теоремата

Нека $N \in \mathbb{N}$ и да означим с $J(N)$ броя на решенията на уравнението

$$p_1 + p_2 = N \tag{221}$$

в прости числа p_1, p_2.

Голдбах е изказал следната

Хипотеза 5.16. *За всяко четно $N \geq 4$ имаме $J(N) > 0$, т.е. N се представя като сума на две прости числа.*

Тази хипотеза не е доказана, но са известни резултати, които в известен смисъл са приближения към нея. Интересуващият се читател може да намери подробна информация в някоя от монографиите [12] и [13].

Намирането на нетривиални оценки отгоре за величината $J(N)$ няма отношение към горната хипотеза, но въпреки това представлява интересна и важна задача. Ще докажем следната

Теорема 5.17. *При произволно $N \geq 2$ имаме*

$$J(N) \ll \frac{N}{\log^2 N} \sum_{d|N} \frac{\mu^2(d)}{d}, \tag{222}$$

като константата в знака $\ll$ е абсолютна.

5.4.2 Начало на доказателството

Първо ще отбележим, че при нечетни N твърдението е тривиално. Наистина, в този случай, ако е изпълнено (221), то някое от простите числа p_1, p_2 ще е равно на 2 и тогава за другото ще има най-много една възможна стойност, или ще имаме $J(N) \ll 1$. Освен това, ако оценката (222) е доказана при достатъчно големи N, то като променим, ако това се налага, константата в знака $\ll$, ще получим оценка за всички $N \geq 2$. И така, оттук нататък ще считаме, че N е достатъчно голямо четно число.

Нека z е параметър, който ще изберем по-късно. Засега предполагаме само, че z е достатъчно голямо и удовлетворява

$$z < \sqrt{N}. \tag{223}$$

Полагаме

$$P = \prod_{p \leq z} p. \tag{224}$$

Ако p е просто число от интервала $(z, N-z)$, за което числото $N-p$ също е просто, то произведението $p(N-p)$ е взаимно просто с P. Оттук получаваме

$$J(N) \leq 2z + \sum_{\substack{z<p<N-z \\ N-p \text{ е просто}}} 1 \leq 2z + J_1(N), \tag{225}$$

където

$$J_1(N) = \#\{n \in \mathbb{N} \,:\, n \leq N,\ \ (n(N-n), P) = 1\}.$$

Сега, като използуваме Лема 3.34 (УАТЧ-1), получаваме

$$J_1(N) = \sum_{n \leq N} \sum_{d|(n(N-n),P)} \mu(d). \tag{226}$$

За да получим добра оценка отгоре за $J_1(N)$ трябва първо да заменим сумата по d в горната формула с друга сума, в която на сумационната променлива d да са наложени допълнителни ограничения, така че броят на събираемите да се намали. В параграф 5.3, където изложихме най-простия вариант на решетото на Брун, за тази цел използувахме Лема 5.15. Сега ще приложим решетото на Селберг, което се основава на следната

Лема 5.18. *Нека за всяко $d \in \mathbb{N}$ е определено $\lambda_d \in \mathbb{R}$, като*

$$\lambda_1 = 1. \tag{227}$$

Тогава за всяко $m \in \mathbb{N}$ е в сила неравенството

$$\sum_{d|m} \mu(d) \leq \left(\sum_{d|m} \lambda_d \right)^2. \tag{228}$$

Доказателство. При $m = 1$ неравенството (228) е изпълнено поради условието (227). При $m > 1$ неравенството отново е вярно, тъй от Лема 3.34 (УАТЧ-1) следва, че изразът от лявата страна е равен на нула, а от дясната страна стои неорицателно число.

□

Нека λ_d, $d = 1, 2, 3, \ldots$ са реални числа, като е изпълнено (227). Оттук нататък ще считаме също, че

$$\lambda_d = 0 \qquad \text{при} \qquad d > z. \tag{229}$$

Засега не определяме λ_d при $1 < d \leq z$ и това ще направим по-късно. Като използуваме (226) и приложим към вътрешната сума Лема 5.18, получаваме

$$J_1(N) \leq J_2(N), \tag{230}$$

където

$$J_2(N) = \sum_{n \leq N} \left(\sum_{d|(n(N-n),P)} \lambda_d \right)^2. \tag{231}$$

Извършваме повдигането на квадрат, след което сменяме реда на сумиране и получаваме

$$J_2(N) = \sum_{n \leq N} \sum_{d_1|(n(N-n),P)} \sum_{d_2|(n(N-n),P)} \lambda_{d_1} \lambda_{d_2}$$

$$= \sum_{\substack{d_1|P \\ d_2|P}} \lambda_{d_1} \lambda_{d_2} \; H(N; d_1, d_2), \tag{232}$$

където

$$H(N; d_1, d_2) = \#\{\, n \in \mathbb{N} \,:\, n \leq N, \;\; n(N-n) \equiv 0 \pmod{d_j}, \;\; j = 1, 2 \,\}.$$

Тогава, като вземем предвид определението на най-малко общо кратно на две числа (виж Определение 3.5 (УАТЧ-1)), виждаме, че

$$H(N; d_1, d_2) = \#\{\, n \in \mathbb{N} \,:\, n \leq N, \;\; n(N-n) \equiv 0 \pmod{[d_1, d_2]} \,\}.$$

Да означим

$$\rho(d) = \#\{\ n \in \mathbb{N}\ :\ 1 \le n \le d, \qquad n(N-n) \equiv 0 \pmod{d}\ \}. \tag{233}$$

Тогава от Лема 3.56 (УАТЧ-1) следва

$$H(N; d_1, d_2) = \frac{\rho([d_1, d_2])}{[d_1, d_2]} N + O(\rho([d_1, d_2])),$$

като константата в знака O е абсолютна. Заместваме последният израз в (232) и намираме

$$J_2(N) = \sum_{\substack{d_1 | P \\ d_2 | P}} \lambda_{d_1} \lambda_{d_2} \ \left(\frac{\rho([d_1, d_2])}{[d_1, d_2]} N + O\left(\rho([d_1, d_2]\ ) \right) \right),$$

следователно

$$J_2(N) = NV + O(R), \tag{234}$$

където

$$V = \sum_{\substack{d_1 | P \\ d_2 | P}} \lambda_{d_1} \lambda_{d_2} \, \frac{\rho([d_1, d_2])}{[d_1, d_2]} \tag{235}$$

$$R = \sum_{\substack{d_1 | P \\ d_2 | P}} |\lambda_{d_1}|\, |\lambda_{d_2}|\, \rho([d_1, d_2]). \tag{236}$$

Нашата цел е да намерим колкото се може по-добра оценка отгоре за $J_2(N)$ и затова трябва да оценим величините V и R. Благодарение на въвеждането на условието (229) избягваме основната пречка, която възниква при прилагането на решетото на Ератостен–Льожандър, а именно наличието на твърде много събираеми в сумата R.

Стойностите на числата λ_d при $1 < d \le z$ все още не са определени. Ние ще ги определим по такъв начин, че величината V да придобие минимална стойност. След това, за вече избраните λ_d ще оценим R.

5.4.3 Минимизиране на величината V.

Първо да отбележим, че поради условието (229) в сумата V, зададена чрез (235), се сумира само по d_1 и d_2 ненадминаващи z. Освен това, от определението (224) на P следва, че делителите на това число са безквадратни. Обратно, ако едно число е безквадратно и не надхвърля z, то непременно ще дели P. Оттук се вижда, че сумата V може да се запише във вида

$$V = \sum_{d_1, d_2 \le z} \lambda_{d_1} \lambda_{d_2}\, \mu^2(d_1) \mu^2(d_2)\, \frac{\rho([d_1, d_2])}{[d_1, d_2]} \tag{237}$$

Намирането на значения на λ_d при $1 < d \leq z$, за които V придобива най-малка стойност, както и изчисляването на тази стойност, е задача за минимизиране на квадратична форма. Добре известно е, че най-удобни за изследване са диагоналните квадратични форми и поради това първо чрез подходяща смяна на променливите ще приведем формата V в диагонален вид.

Ще използуваме следната лема, чието елементарно доказателство оставяме на читателя.

Лема 5.19. *Нека f е мултипликативна функция. Тогава за произволни $n_1, n_2 \in \mathbb{N}$ имаме*

$$f([n_1, n_2])f((n_1, n_2)) = f(n_1)f(n_2),$$

където $[n_1, n_2]$ и (n_1, n_2) са съответно най-малкото общо кратно и най-големия общ делител на n_1, n_2.

□

Вследствие на Лема 3.56 (УАТЧ-1) функцията $\rho(d)$, определена чрез (233), е мултипликативна, следователно

$$\rho(d) = \prod_{p|d} \rho(p) \qquad \text{при} \qquad \mu^2(d) = 1. \tag{238}$$

Освен това, непосредствено се вижда, че за всяко просто число p е изпълнено

$$\rho(p) = \begin{cases} 1 & \text{при} \quad p \mid N, \\ 2 & \text{при} \quad p \nmid N. \end{cases} \tag{239}$$

От горните формули следва, в частност, че

$$\rho(d) \geq 1 \qquad \text{при} \qquad \mu^2(d) = 1. \tag{240}$$

Тогава, като използуваме Лема 5.19, получаваме

$$\frac{\rho([d_1, d_2])}{[d_1, d_2]} = \frac{\rho(d_1)}{d_1} \frac{\rho(d_2)}{d_2} \frac{(d_1, d_2)}{\rho((d_1, d_2))}.$$

Заместваме този израз в (237) и намираме

$$V = \sum_{d_1, d_2 \leq z} \frac{\lambda_{d_1} \mu^2(d_1) \rho(d_1)}{d_1} \frac{\lambda_{d_2} \mu^2(d_2) \rho(d_2)}{d_2} \frac{(d_1, d_2)}{\rho((d_1, d_2))}. \tag{241}$$

Сега използуваме Лема 3.37 (УАТЧ-1) и определяме аритметична функция h чрез равенството

$$\sum_{t|n} h(t) = \frac{n\, \mu^2(n)}{\rho(n)}. \tag{242}$$

При това тази функция е мултипликативна, тъй като функцията в дясната страна на (242) е такава. От (242) се вижда, че ако p е просто число, то

$$1 + h(p) = \frac{p}{\rho(p)}$$

и от горното равенство и (239) следва

$$h(p) = \frac{p - \rho(p)}{\rho(p)} > 0. \tag{243}$$

(Тук използуваме, че числото N е четно, следователно $\rho(2) = 1$). От (243) получаваме също

$$h(t) = \prod_{p|t} h(p) > 0 \qquad \text{при} \qquad \mu^2(t) = 1. \tag{244}$$

Като използуваме (241) и (242) записваме V във вида

$$V = \sum_{d_1, d_2 \le z} \frac{\lambda_{d_1} \mu^2(d_1) \rho(d_1)}{d_1} \frac{\lambda_{d_2} \mu^2(d_2) \rho(d_2)}{d_2} \sum_{t|(d_1, d_2)} h(t).$$

Сега сменяме реда на сумиране и получаваме

$$V = \sum_{t \le z} \mu^2(t) h(t) \sum_{\substack{d_1, d_2 \le z \\ t|d_1,\ t|d_2}} \frac{\lambda_{d_1}\, \mu^2(d_1)\, \rho(d_1)}{d_1} \frac{\lambda_{d_2}\, \mu^2(d_2)\, \rho(d_2)}{d_2}$$

$$= \sum_{t \le z} \mu^2(t)\, h(t)\, U_t^2, \tag{245}$$

където

$$U_t = \sum_{\substack{d \le z \\ t|d}} \frac{\lambda_d\, \mu^2(d)\, \rho(d)}{d}. \tag{246}$$

Да отбележим, че от (229) и (246) следва, че

$$U_t = 0 \qquad \text{при} \qquad t > z. \tag{247}$$

И така, виждаме, че чрез смяната на променливите λ_d с новите променливи U_t, определени чрез (246), привеждаме квадратичната форма V в диагонален вид. При това, от (244) следва, че нашата квадратична форма е положително определена.

Следващата лема дава възможност да изразим променливите λ_d чрез U_t.

Лема 5.20. *Нека $f(n)$ и $g(n)$ са аритметични функции, които се анулират за достатъчно големи стойности на n. Тогава следните две формули са еквивалентни:*

$$g(n) = \sum_{d=1}^{\infty} f(dn) \tag{248}$$

$$f(n) = \sum_{d=1}^{\infty} \mu(d) g(dn). \tag{249}$$

Доказателство. Нека е изпълнено (248). Тогава

$$\sum_{d=1}^{\infty}\mu(d)g(dn)=\sum_{d=1}^{\infty}\mu(d)\sum_{m=1}^{\infty}f(mdn)=\sum_{d=1}^{\infty}\sum_{m=1}^{\infty}\mu(d)f(mdn)$$

$$=\sum_{k=1}^{\infty}\sum_{\substack{d=1\\ md=k}}^{\infty}\sum_{m=1}^{\infty}\mu(d)f(mdn)=\sum_{k=1}^{\infty}f(kn)\sum_{md=k}\mu(d). \tag{250}$$

Но от Лема 3.34 (УАТЧ-1) знаем, че

$$\sum_{md=k}\mu(d)=\sum_{d|k}\mu(d)=\begin{cases}1 & \text{при} \quad k=1,\\ 0 & \text{при} \quad k>1,\end{cases}$$

следователно изразът в дясната страна на (250) е равен на $f(n)$, т.е. получихме (249). По аналогичен начин се показва, че от (249) следва (248). Проверката оставяме на читателя.

□

За да приложим Лема 5.20 полагаме

$$\eta_d=\begin{cases}1 & \text{при} \quad d\le z,\\ 0 & \text{в противен случай}\end{cases} \tag{251}$$

и

$$f(d)=\eta_d\,\frac{\lambda_d\,\mu^2(d)\,\rho(d)}{d}. \tag{252}$$

Тогава от (246) получаваме

$$U_t=\sum_{\substack{d=1\\ t|d}}^{\infty}f(d)=\sum_{d=1}^{\infty}f(dt)$$

и от Лема 5.20 следва

$$f(d)=\sum_{t=1}^{\infty}\mu(t)\,U_{dt}. \tag{253}$$

Като използуваме (247) и (251) – (253) получаваме

$$\frac{\lambda_d\,\rho(d)}{d}=\sum_{t\le\frac{z}{d}}\mu(t)\,U_{dt}\qquad\text{при}\qquad d\le z,\qquad \mu^2(d)=1 \tag{254}$$

и, в частност, като вземем предвид (227) виждаме, че

$$1=\lambda_1=\sum_{t\le z}\mu(t)\,U_t. \tag{255}$$

За да продължим по-нататък е необходимо за всяко $t\le z$, за което $\mu^2(t)=1$, да определим U_t така, че да е изпълнено условието (255), а също квадратичната форма V, определена чрез (245), да приема минимална стойност. Ще използуваме следната

Лема 5.21. *Дадени са числата* $\alpha_1, \ldots, \alpha_n; \beta_1, \ldots, \beta_n \in \mathbb{R}$, *като* $\alpha_j > 0$ *за всяко* $j = 1, \ldots, n$ *и* $\beta_j \neq 0$ *за някое* j. *Тогава най-малката стойност на квадратичната форма*

$$f(\mathbf{x}) = \alpha_1 x_1^2 + \cdots + \alpha_n x_n^2 \tag{256}$$

върху хиперповърхнината

$$\beta_1 x_1 + \cdots + \beta_n x_n = 1 \tag{257}$$

е равна на

$$\varkappa = \left(\sum_{j=1}^{n} \alpha_j^{-1} \beta_j^2 \right)^{-1} \tag{258}$$

и се достига в точката $\mathbf{x}$ *с координати*

$$x_j = \varkappa \alpha_j^{-1} \beta_j, \qquad j = 1, \ldots, n. \tag{259}$$

Доказателство. От неравенството на Коши и от (256) – (258) следва, че върху хиперравнината (257) е изпълнено

$$1 = \left(\sum_{j=1}^{n} \beta_j x_j \right)^2 = \left(\sum_{j=1}^{n} \left(\alpha_j^{-\frac{1}{2}} \beta_j \right) \left(\alpha_j^{\frac{1}{2}} x_j \right) \right)^2$$

$$\leq \left(\sum_{j=1}^{n} \alpha_j^{-1} \beta_j^2 \right) \left(\sum_{j=1}^{n} \alpha_j x_j^2 \right)$$

$$= \varkappa^{-1} f(\mathbf{x}).$$

Следователно за всяко $\mathbf{x}$, удовлетворяващо (257) имаме $f(\mathbf{x}) \geq \varkappa$. Равенство ще се достига точно когато за някое $\gamma \in \mathbb{R}$ е изпълнено

$$\alpha_j^{\frac{1}{2}} x_j = \gamma \alpha_j^{-\frac{1}{2}} \beta_j \qquad \text{при} \qquad j = 1, \ldots, n.$$

Но тогава от (257) и (258) следва, че $\gamma = \varkappa$, с което лемата е доказана.

□

Да продължим с изследването на величината V. Като използуваме (244), (245), (255) и Лема 5.21 виждаме, че

$$V \geq W^{-1},$$

където

$$W = \sum_{n \leq z} \frac{\mu^2(n)}{h(n)}. \tag{260}$$

Тази минимална стойност на V се достига когато изберем

$$U_t = W^{-1} \frac{\mu(t)}{h(t)} \qquad \text{при} \qquad t \leq z, \tag{261}$$

така че в този случай ще имаме

$$V = W^{-1}. \tag{262}$$

5.4.4 Оценяване на R.

Заместваме във формула (254) величините U_t с техните стойности, определени от (261) и намираме, че при $d \le z$, $\mu^2(d) = 1$ е изпълнено

$$\lambda_d = \frac{d}{\rho(d)} \sum_{n \le \frac{z}{d}} \mu(n)\, U_{nd} = \frac{d}{\rho(d)} \sum_{n \le \frac{z}{d}} \mu(n)\, \frac{\mu(nd)}{h(nd)}\, W^{-1} = \frac{d\,\mu(d)}{\rho(d)h(d)}\, \frac{W_d}{W}, \tag{263}$$

където

$$W_d = \sum_{\substack{n \le \frac{z}{d} \\ (n,d)=1}} \frac{\mu^2(n)}{h(n)} \tag{264}$$

От (244), (260) и (264) виждаме, че

$$0 < W_d \le W$$

и от последната формула и (263) получаваме

$$|\lambda_d| \le \frac{d}{\rho(d)h(d)} \qquad \text{при} \qquad d \le z, \qquad \mu^2(d) = 1. \tag{265}$$

Сега ще оценим сумата R, определена чрез (236). Първо забелязваме, че вследствие на (240) и Лема 5.19 имаме

$$\rho([d_1, d_2]) = \frac{\rho(d_1)\rho(d_1)}{\rho((d_1, d_2))} \le \rho(d_1)\rho(d_1) \qquad \text{при} \qquad \mu^2(d_1) = \mu^2(d_2) = 1.$$

Използуваме също (224) и съображението, приведено в началото на параграф 5.4.3, и получаваме

$$R \le \sum_{d_1, d_2 \le z} |\lambda_{d_1}|\, |\lambda_{d_2}|\, \mu^2(d_1)\, \mu^2(d_2)\, \rho(d_1)\, \rho(d_1) = K^2, \tag{266}$$

където

$$K = \sum_{d \le z} |\lambda_d|\, \mu^2(d)\, \rho(d). \tag{267}$$

От (265) и (267) следва

$$K \le \sum_{d \le z} \frac{d\mu^2(d)}{h(d)}. \tag{268}$$

За да оценим величината K забелязваме, че от (239), (243), (244), както и Леми 3.32, 3.33 (УАТЧ-1) следва, че при $\mu^2(d) = 1$ имаме

$$\frac{d}{h(d)} = \prod_{p \mid d} \frac{p\rho(p)}{p - \rho(p)} \le \prod_{p \mid d} 8 = \tau^3(d) \ll d^{\varepsilon},$$

където $\varepsilon > 0$ е произволно малко, а константата в знака $\ll$ зависи от ε. От последната формула и от (268) получаваме

$$K \ll z^{1+\varepsilon}.$$

Сега, като заместим в (266) виждаме, че

$$R \ll z^{2+\varepsilon}, \tag{269}$$

където $\varepsilon > 0$ е произволно малко, а константата в знака $\ll$ зависи от ε.

5.4.5 Оценка отдолу за W и край на доказателството

Като използуваме (225), (230), (234), (262) и (269) получаваме

$$J(N) \ll NW^{-1} + z^{2+\varepsilon}, \tag{270}$$

където W се определя от (260). За да довършим доказателството ще оценим отдолу W, след което ще изберем по подходящ начин параметъра z.

Определяме аритметичните функции $\xi(n)$ и $H(n)$ по следния начин. Полагаме $\xi(1) = H(1) = 1$. Ако $n > 1$ притежава канонично разлагане $n = p_1^{\alpha_1} \dots p_s^{\alpha_s}$, то

$$\xi(n) = p_1 \dots p_s, \tag{271}$$

$$H(n) = \rho(p_1)^{\alpha_1} \dots \rho(p_s)^{\alpha_s}, \tag{272}$$

където $\rho(d)$ се определя от (233). Очевидно, тези две функции са мултипликативни. Ако $h(d)$ е функцията, зададена чрез (243) и (244), то

$$\frac{\mu^2(d)}{h(d)} = \mu^2(d) \prod_{p|d} \left(\frac{\rho(p)}{p} \left(1 - \frac{\rho(p)}{p} \right)^{-1} \right)$$

$$= \mu^2(d) \prod_{p|d} \left(\frac{\rho(p)}{p} + \frac{\rho^2(p)}{p^2} + \frac{\rho^3(p)}{p^3} + \dots \right).$$

Умножаваме редовете в последното произведение и като използуваме (271) и (272), получаваме

$$\frac{\mu^2(d)}{h(d)} = \mu^2(d) \sum_{\substack{n \in \mathbb{N} \\ \xi(n) = d}} \frac{H(n)}{n}.$$

От последното тъждество и от (260) следва

$$W = \sum_{d \le z} \mu^2(d) \sum_{\substack{n \in \mathbb{N} \\ \xi(n) = d}} \frac{H(n)}{n}.$$

Сменяме реда на сумиране, виждаме, че

$$W = \sum_{\substack{n \in \mathbb{N} \\ \xi(n) \le z}} \frac{H(n)}{n} \sum_{\substack{d \le z \\ d = \xi(n)}} \mu^2(d) = \sum_{\substack{n \in \mathbb{N} \\ \xi(n) \le z}} \frac{H(n)}{n} \ge \sum_{n \le z} \frac{H(n)}{n}. \tag{273}$$

Сега определяме аритметична функция $V(n)$ по следния начин. Нека $V(1) = 1$. Ако $n > 1$ притежава канонично разлагане $n = p_1^{\alpha_1} \dots p_s^{\alpha_s} q_1^{\beta_1} \dots q_t^{\beta_t}$, където $p_i \mid N$, а $q_j \nmid N$, полагаме

$$V(n) = (1 + \beta_1) \dots (1 + \beta_t). \tag{274}$$

От (239), (272) и (274) получаваме

$$H(n) \geq V(n)$$

и, като използуваме (273), виждаме, че

$$W \geq \sum_{n \leq z} \frac{V(n)}{n}. \tag{275}$$

Ако $\varphi(n)$ е функцията на Ойлер (виж Определение 3.20 (УАТЧ-1)), то като приложим Лема 3.40 (УАТЧ-1), намираме

$$\frac{N}{\varphi(N)} = \prod_{p|N} \left(1 - \frac{1}{p}\right)^{-1} = \prod_{p|N} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \dots\right)$$

Умножаваме редовете в последното произведение и получаваме

$$\frac{N}{\varphi(N)} = \sum_{\substack{m \in \mathbb{N} \\ p|m \Rightarrow p|N}} \frac{1}{m}. \tag{276}$$

От (275) и (276) следва

$$\frac{N}{\varphi(N)} W \geq \sum_{n \leq z} \frac{V(n)}{n} \sum_{\substack{m \in \mathbb{N} \\ p|m \Rightarrow p|N}} \frac{1}{m} = \sum_{n \leq z} V(n) \sum_{\substack{m \in \mathbb{N} \\ p|m \Rightarrow p|N}} \frac{1}{mn} = \sum_{n \leq z} V(n) \sum_{\substack{h \in \mathbb{N} \\ h \equiv 0 \pmod{n} \\ p|\frac{h}{n} \Rightarrow p|N}} \frac{1}{h}.$$

Сменяме реда на сумиране в последния израз и получаваме

$$\frac{N}{\varphi(N)} W \geq \sum_{h=1}^{\infty} \frac{1}{h} \sum_{\substack{n \leq z \\ n|h \\ p|\frac{h}{n} \Rightarrow p|N}} V(n) \geq \sum_{h \leq z} \frac{1}{h} \sum_{\substack{n|h \\ p|\frac{h}{n} \Rightarrow p|N}} V(n). \tag{277}$$

Сега ще намерим по-прост вид за вътрешната сума в израза от дясната страна на последното неравенство, като за целта ще използуваме определението на $V(n)$, дадено чрез (274). Нека $h > 1$ притежава канонично разлагане

$$h = p_1^{\alpha_1} \dots p_s^{\alpha_s} q_1^{\beta_1} \dots q_t^{\beta_t}, \qquad \text{където} \qquad p_i \mid N, \qquad q_j \nmid N.$$

Ако n е делител на h, такъв че всеки прост делител на $\frac{h}{n}$ дели също N, то

$$n = p_1^{\gamma_1} \dots p_s^{\gamma_s} q_1^{\beta_1} \dots q_t^{\beta_t}, \qquad \text{където} \qquad 0 \leq \gamma_i \leq \alpha_i, \qquad i = 1, \dots, s.$$

Тогава ще имаме

$$V(n) = (1 + \beta_1) \dots (1 + \beta_t).$$

От горната формула и от Лема 3.32 (УАТЧ-1) следва, че

$$\sum_{\substack{n|h \\ p|\frac{h}{n} \Rightarrow p|N}} V(n) = \sum_{\gamma_1=0}^{\alpha_1} \cdots \sum_{\gamma_s=0}^{\alpha_s} (1+\beta_1)\ldots(1+\beta_t)$$

$$= (1+\alpha_1)\ldots(1+\alpha_s)(1+\beta_1)\ldots(1+\beta_t)$$

$$= \tau(h).$$

Очевидно горното равенство е вярно и при $h = 1$.

Заместваме получения израз в (277) и намираме

$$\frac{N}{\varphi(N)} W \geq \sum_{h \leq z} \frac{\tau(h)}{h}. \tag{278}$$

По-нататък, като използуваме Лема 2.6 и Определение 3.17 (УАТЧ-1) виждаме, че

$$\sum_{h \leq z} \frac{\tau(h)}{h} = \sum_{uv \leq z} \frac{1}{uv} \geq \sum_{u,v \leq \sqrt{z}} \frac{1}{uv} = \left(\sum_{u \leq \sqrt{z}} \frac{1}{u} \right)^2 \gg \log^2 z. \tag{279}$$

От (278) и (279) получаваме

$$W \gg \frac{\varphi(N)}{N} \log^2 z. \tag{280}$$

Използуваме оценките (270) и (280) и виждаме, че

$$J(N) \ll \frac{N^2}{\varphi(N) \log^2 z} + z^{2+\varepsilon}.$$

Сега избираме

$$z = N^{\frac{1}{3}}$$

и получаваме

$$J(N) \ll \frac{N^2}{\varphi(N) \log^2 N}. \tag{281}$$

Остава да забележим, че вследствие на Лема 3.40 (УАТЧ-1) имаме

$$\frac{N}{\varphi(N)} = \prod_{p|N} \left(1 - \frac{1}{p}\right)^{-1} = \prod_{p|N} \left(1 - \frac{1}{p^2}\right)^{-1} \prod_{p|N} \left(1 + \frac{1}{p}\right). \tag{282}$$

Изпълнено е също

$$\prod_{p|N} \left(1 - \frac{1}{p^2}\right)^{-1} \leq \prod_{p} \left(1 - \frac{1}{p^2}\right)^{-1} = \frac{\pi^2}{6} \ll 1 \tag{283}$$

(виж доказателството на Лема 3.59 (УАТЧ-1)). Накрая, очевидно е, че

$$\prod_{p|N}\left(1+\frac{1}{p}\right)=\sum_{k|N}\frac{\mu^2(k)}{k}. \tag{284}$$

От (281) – (284) следва

$$J(N)\ll\frac{N}{\log^2 N}\sum_{k|N}\frac{\mu^2(k)}{k},$$

с което теоремата е доказана.

□

6 Метод на Шнирелман в адитивната теория на числата

6.1 Плътност на редица от естествени числа

В настоящата глава ще означаваме с $\mathbb{N}_0$ множеството на неотрицателните цели числа, т.е.

$$\mathbb{N}_0 = \mathbb{N} \cup \{0\}.$$

Нека $\mathcal{A} \subset \mathbb{N}_0$. За всяко $n \in \mathbb{N}$ означаваме с $D_{\mathcal{A}}(n)$ броя на естествените числа от $\mathcal{A}$, които не надминават n, т.е.

$$D_{\mathcal{A}}(n) = \#\{a \in \mathcal{A} \ : \ 1 \leq a \leq n\}. \tag{285}$$

Очевидно винаги е изпълнено $0 \leq D_{\mathcal{A}}(n) \leq n$. Това неравенство ни дава възможност да дадем следното

Определение 6.1. *Плътност на Шнирелман на множеството $\mathcal{A} \subset \mathbb{N}_0$ наричаме числото*

$$d(\mathcal{A}) = \inf_{n \in \mathbb{N}} \frac{D_{\mathcal{A}}(n)}{n}. \tag{286}$$

Например, ако

$$\mathcal{A} = \{0,\ 1,\ 1+r,\ 1+2r,\ 1+3r, \dots\},$$

където $r \in \mathbb{N}$, то $d(\mathcal{A}) = \frac{1}{r}$.

Ако пък

$$\mathcal{A}^{(k)} = \{0,\ 1^k,\ 2^k,\ 3^k,\ 4^k, \dots\}, \tag{287}$$

където $k \in \mathbb{N}$, $k \geq 2$, то $d(\mathcal{A}^{(k)}) = 0$. Елементарната проверка на горните равенства оставяме на читателя.

От Определение (6.1) непосредствено следва

Лема 6.2. *Ако $\mathcal{A}$, $\mathcal{B} \subset \mathbb{N}_0$, то са в сила следните твърдения:*

(1) *Ако $\mathcal{A}$ е крайно, то $d(\mathcal{A}) = 0$.*

(2) *Винаги е изпълнено $0 \leq d(\mathcal{A}) \leq 1$.*

(3) *Ако $\mathcal{A} \subset \mathcal{B}$, то $d(\mathcal{A}) \leq d(\mathcal{B})$.*

(4) *Ако $1 \notin \mathcal{A}$, то $d(\mathcal{A}) = 0$.*

Доказателство. Свойства (1), (2) и (3) са очевидни, а за да установим (4) е достатъчно да забележим, че ако $1 \notin \mathcal{A}$, то $D_{\mathcal{A}}(1) = 0$.

□

В адитивната теория на числата основна роля играе следното

Определение 6.3. *Ако $\mathcal{A}_1, \ldots, \mathcal{A}_k \subset \mathbb{N}_0$, то сума на тези множества наричаме множеството*

$$\mathcal{A}_1 + \cdots + \mathcal{A}_k = \{a_1 + \cdots + a_k \ : \ a_1 \in \mathcal{A}_1, \ldots, a_k \in \mathcal{A}_k\}. \tag{288}$$

Това определение ни дава възможност да формулираме адитивните задачи като съотношения между числови множества. Например, ако $\mathcal{A}^{(k)}$ е определно чрез (287), то теоремата на Лагранж за представимостта на числата като сума от четири квадрата (виж (УАТЧ-1), Глава 3) е еквивалента на равенството

$$\mathcal{A}^{(2)} + \mathcal{A}^{(2)} + \mathcal{A}^{(2)} + \mathcal{A}^{(2)} = \mathbb{N}_0.$$

По подобен начин може да се формулира и известния проблем на Варинг (виж, например, монографиите на Карацуба [4], Вон [22], както и записките на автора [6]).

Интуицията ни подсказва, че ако едно множество има достатъчно голяма плътност, то събирайки го известен брой пъти само със себе си (по правилото от формула (288)), ще покрием множеството на естествените числа. Следващите леми потвърждават това предположение.

Ще започнем със следната

Лема 6.4. *Дадено е множеството $\mathcal{A} \subset \mathbb{N}_0$, за което $0 \in \mathcal{A}$ и $d(\mathcal{A}) \geq \frac{1}{2}$. Тогава е изпълнено*

$$\mathcal{A} + \mathcal{A} = \mathbb{N}_0.$$

Доказателство. Нека ненулевите елементи на $\mathcal{A}$, наредени по големина, са

$$0 < a_1 < a_2 < a_3 < \ldots.$$

Взимаме произволно $n \in \mathbb{N}$. Ще установим, че е изпълнено $n \in \mathcal{A}$, или пък $n = a_i + a_j$ за някои i, j и с това лемата ще бъде доказана.

Означаваме с k най-големия индекс, за който $a_k \leq n$.

Ако $a_k = n$, то $n \in \mathcal{A}$.

Нека сега предположим, че $a_k < n$. Тогава от (285) следва, че $D_{\mathcal{A}}(n) = k$. Тъй като по условие имаме $d(\mathcal{A}) \geq \frac{1}{2}$, то като използуваме Определение 6.1, виждаме, че

$$k = D_{\mathcal{A}}(n) \geq \frac{n}{2}. \tag{289}$$

Да разгледаме множествата

$$\mathcal{I} = \{a_1, a_2, \ldots, a_k\}, \qquad \mathcal{J} = \{n - a_1, n - a_2, \ldots, n - a_k\},$$

за които очевидно имаме

$$\#\mathcal{I} = \#\mathcal{J} = k.$$

Ако допуснем, че тези множества не се пресичат, то, като вземем предвид (289), намираме

$$\#(\mathcal{I} \cup \mathcal{J}) = 2k \geq n.$$

От друга страна, множеството $\mathcal{I} \cup \mathcal{J}$ се състои от естествени числа, ненадминаващи $n - 1$, следователно

$$\#(\mathcal{I} \cup \mathcal{J}) \leq n - 1.$$

Тъй като последните две неравенства не могат да са едновременно верни, то виждаме, че $\mathcal{I} \cap \mathcal{J} \neq \emptyset$. Следователно съществуват индекси i, j, за които $a_i = n - a_j$, т.е. $n = a_i + a_j$. С това лемата е доказана.

□

Следващата лема ни дава връзка между плътностите на две множества и плътността на тяхната сума.

Лема 6.5. *Дадени са множествата $\mathcal{A}, \mathcal{B} \subset \mathbb{N}_0$, за които $0 \in \mathcal{A} \cap \mathcal{B}$. Тогава имаме*

$$d(\mathcal{A} + \mathcal{B}) \geq d(\mathcal{A}) + d(\mathcal{B}) - d(\mathcal{A})d(\mathcal{B}). \tag{290}$$

Доказателство. Полагаме

$$\alpha = d(\mathcal{A}), \qquad \beta = d(\mathcal{B}), \qquad \gamma = d(\mathcal{A} + \mathcal{B}). \tag{291}$$

Да допуснем, че $\alpha = 0$. От условието $0 \in \mathcal{A}$ следва, че $\mathcal{A} + \mathcal{B} \supset \mathcal{B}$ и, като използуваме Лема 6.2 (3), получаваме $\gamma \geq \beta$, което означава, че в този случай (290) е вярно. Аналогично разсъждаваме и в случая $\beta = 0$.

Оттук нататък ще считаме, че $\alpha > 0$ и $\beta > 0$. Тогава от Лема 6.2 (4) следва, че $1 \in \mathcal{A} \cap \mathcal{B}$. Нека ненулевите елементи на множествата $\mathcal{A}$ и $\mathcal{B}$ са

$$1 = a_1 < a_2 < a_3 < \ldots$$

и съответно

$$1 = b_1 < b_2 < b_3 < \ldots.$$

От Определение 6.1 и от (291) следва, че за всяко $n \in \mathbb{N}$ е изпълнено

$$D_{\mathcal{A}}(n) \geq \alpha n, \qquad D_{\mathcal{B}}(n) \geq \beta n. \tag{292}$$

За да докажем (290) ще оценим отдолу $D_{\mathcal{A}+\mathcal{B}}(m)$ за произволно $m \in \mathbb{N}$. Ако k е най-голямото естествено число, за което $a_k \leq m$, то имаме

$$D_{\mathcal{A}}(m) = k. \tag{293}$$

По условие имаме $0 \in \mathcal{B}$, следователно интервалът $[1, m]$ съдържа поне k на брой числа от $\mathcal{A}+\mathcal{B}$, а именно $a_1, a_2, \ldots, a_k$. Освен тези, ще намерим и други елементи на $\mathcal{A}+\mathcal{B}$, лежащи в същия интервал, като разсъждаваме по следния начин.

Във всеки от интервалите

$$(a_{\nu-1}, a_\nu), \qquad 2 \leq \nu \leq k$$

се намират числата

$$a_{\nu-1} + b_1,\ a_{\nu-1} + b_2,\ \ldots,\ a_{\nu-1} + b_{i_{\nu-1}},$$

където $i_{\nu-1}$ е най-големият индекс, за който $a_{\nu-1} + b_{i_{\nu-1}} \leq a_\nu - 1$. Тогава, като вземем предвид (285) и (292) виждаме, че

$$i_{\nu-1} = D_{\mathcal{B}}(a_\nu - a_{\nu-1} - 1) \geq \beta(a_\nu - a_{\nu-1} - 1), \qquad 2 \leq \nu \leq k. \tag{294}$$

Освен това, ако $a_k < m$, то в интервала $(a_k, m]$ се намират числата

$$a_k + b_1,\ a_k + b_2,\ \ldots,\ a_k + b_{i_k},$$

където i_k е най-големият индекс, удовлетворяващ $a_k + b_{i_k} \leq m$. Оттук и от (285), (292) следва, че

$$i_k = D_{\mathcal{B}}(m - a_k) \geq \beta(m - a_k). \tag{295}$$

Ако пък $a_k = m$, полагаме $i_k = 0$ и последното неравенство отново е вярно.

От горните съображения и от (292) – (295) получаваме

$$\begin{aligned}
D_{\mathcal{A}+\mathcal{B}}(m) &\geq k + \sum_{\nu=2}^{k} i_{\nu-1} + i_k \\
&\geq k + \sum_{\nu=2}^{k} \beta(a_\nu - a_{\nu-1} - 1) + \beta(m - a_k) \\
&= k + \beta(m - a_1 - (k-1)) \\
&= (1-\beta)k + \beta m \\
&= (1-\beta)D_{\mathcal{A}}(m) + \beta m \\
&\geq (1-\beta)\alpha m + \beta m \\
&= (\alpha + \beta - \alpha\beta)m.
\end{aligned}$$

От горното неравенство и от Определение 6.1 получаваме

$$\gamma = \inf_{m\in\mathbb{N}} \frac{D_{\mathcal{A}+\mathcal{B}}(m)}{m} \geq \alpha + \beta - \alpha\beta,$$

с което лемата е доказана.

□

Да отбележим, че е в сила и по-силен резултат, от изложения в Лема 6.5. Поточно, при същите условия е изпълнено

$$d(\mathcal{A}+\mathcal{B}) \geq \min\left(1, d(\mathcal{A}) + d(\mathcal{B})\right)$$

Това неравенство е установено от Х. Ман през 1942 г. Подробно доказателство е изложено в първа глава на монографията [5] на Гелфонд и Линник. За нашите цели обаче е достатъчно да се възползуваме от неравенството (290).

От Лема 6.5 получаваме

Следствие 6.6. *Дадени са множествата* $\mathcal{A}_1, \ldots, \mathcal{A}_r \subset \mathbb{N}_0$, *за които* $0 \in \bigcap_{\nu=1}^{r} \mathcal{A}_\nu$. *Тогава е в сила неравенството*

$$1 - d(\mathcal{A}_1 + \ldots \mathcal{A}_r) \leq (1 - d(\mathcal{A}_1)) \ldots (1 - d(\mathcal{A}_r)). \tag{296}$$

Доказателство. При $r = 1$ твърдението е тривиално, а при $r = 2$ следва непосредствено от Лема 6.5. Нека разгледаме случая $r \geq 3$. Да положим

$$\mathcal{B}_\nu = \mathcal{A}_1 + \cdots + \mathcal{A}_\nu, \qquad 1 \leq \nu \leq r-1$$

и да допуснем, че в случая $\nu \leq r-1$ е изпълнено

$$1 - d(\mathcal{B}_\nu) \leq (1 - d(\mathcal{A}_1)) \ldots (1 - d(\mathcal{A}_\nu)).$$

Тъй като $\mathcal{B}_{\nu+1} = \mathcal{B}_\nu + \mathcal{A}_{\nu+1}$, то от Лема 6.5 и от индукционното предположение следва

$$1 - d(\mathcal{B}_{\nu+1}) \leq (1 - d(\mathcal{B}_\nu))(1 - d(\mathcal{A}_{\nu+1})) \leq (1 - d(\mathcal{A}_1)) \ldots (1 - d(\mathcal{A}_{\nu+1})).$$

Тогава (296) е изпълнено за произволно r и лемата е доказана.

□

Като използуваме Следствие 6.6 получаваме

Лема 6.7. *Дадено е множеството* $\mathcal{A} \subset \mathbb{N}_0$, *за което* $0 \in \mathcal{A}$ *и* $d(\mathcal{A}) > 0$. *Означаваме*

$$\mathcal{B}_k = \underbrace{\mathcal{A} + \cdots + \mathcal{A}}_{k \text{ пъти}}.$$

Тогава съществува $k \in \mathbb{N}$ *такова, че* $\mathcal{B}_k = \mathbb{N}_0$.

Доказателство. Означаваме $\alpha = d(\mathcal{A})$ и, като използуваме Следствие 6.6 виждаме, че за произволно $l \in \mathbb{N}$ е изпълнено

$$1 - d(\mathcal{B}_l) \leq (1-\alpha)^l. \tag{297}$$

Тъй като по условие $\alpha > 0$, можем да изберем l така, че $(1-\alpha)^l \leq \frac{1}{2}$ и тогава, като вземем предвид (297), ще имаме $d(\mathcal{B}_l) \geq \frac{1}{2}$. Сега, като използуваме Лема 6.4, виждаме, че

$$\mathcal{B}_{2l} = \mathcal{B}_l + \mathcal{B}_l = \mathbb{N}_0,$$

с което лемата е доказана.

□

6.2 Теорема на Шнирелман за представяне на числата като суми от прости числа

6.2.1 Формулировка на теоремата

Ще докажем следната

Теорема 6.8 (Шнирелман, 1931)**.** *Съществува константа k_0 такава, че всяко естествено число $N > 1$ може да се представи като сума на не повече от k_0 на брой прости числа.*

Константата k_0 е известна като *константа на Шнирелман* и той е установил, че $k_0 \leq 800000$. Да отбележим, че през 1937 г. И. М. Виноградов е доказал, че всяко достатъчно голямо нечетно число може да се представи като сума на три прости числа (виж монографиите на Карацуба [4], Вон [22], или пък записките на автора [6]). Оттук следва, че съществува N_0 такова, че всяко естествено число $N \geq N_0$ може да се представи като сума на не-повече от 4 прости числа.

Стойността на N_0, която се получава като се следват аргументите на Виноградов, е изключително голямо число и в продължение на много години редица математици се опитваха да докажат представимостта и на нечетните числа по-малки от N_0 като сума на три прости числа. Ще отбележим, че за тази цел е нужно да бъдат предолени сериозни препятствия, включително и от теоретичен характер. С тази задача едва през май 2013 г. се справи Хелфгот [15], [16] и в настоящия момент тернарната хипотеза на Голдбах, според която всяко нечетно число по-голямо от 5 е сума на три прости числа, е напълно доказана. Оттук веднага следва, че за константата на Шнирелман имаме $k_0 \leq 4$. В настоящите записки обаче няма да се занимаваме с тези въпроси и ще насочим вниманието си към доказателството на Теорема 6.8.

6.2.2 Някои леми

Основна роля в доказателството на Теорема 6.8 играе следната

Лема 6.9. *Ако $J(n)$ е броя на представянията на естественото число n като сума на две прости числа, то за всяко $x \geq 2$ е в сила оценката*

$$\sum_{n \leq x} J^2(n) \ll \frac{x^3}{\log^4 x}. \tag{298}$$

Доказателство. Да означим с F сумата в лявата страна на (298) Използуваме оценката за $J(n)$ от Теорема 5.17 и виждаме, че

$$F \ll \sum_{1<n\le x} \frac{n^2}{\log^4 n} \sum_{\substack{k_1|n\\ k_2|n}} \frac{\mu^2(k_1)}{k_1}\frac{\mu^2(k_2)}{k_2} \ll \frac{x^2}{\log^4 x} \sum_{n\le x} \sum_{\substack{k_1|n\\ k_2|n}} \frac{1}{k_1k_2}.$$

Сега сменяме реда на сумиране и използуваме определението за най-малко общо кратно. Получаваме

$$F \ll \frac{x^2}{\log^4 x} \sum_{k_1,k_2\le x} \frac{1}{k_1k_2} \sum_{\substack{n\le x\\ n\equiv 0 \pmod{[k_1,k_2]}}} 1 = \frac{x^2}{\log^4 x} \sum_{k_1,k_2\le x} \frac{1}{k_1k_2}\,\frac{x}{[k_1,k_2]}.$$

Оттук следва

$$F \ll \frac{x^3}{\log^4 x}\, F_1, \qquad \text{където} \qquad F_1 = \sum_{k_1,k_2\le x} \frac{1}{k_1k_2[k_1,k_2]}. \tag{299}$$

За да оценим F_1 използуваме формулата $[k_1,k_2](k_1,k_2) = k_1k_2$ (виж Лема 5.19), както и очевидното неравенство $(k_1,k_2) \le \min(k_1,k_2) \le \sqrt{k_1k_2}$ и получаваме

$$F_1 = \sum_{k_1,k_2\le x} \frac{(k_1,k_2)}{k_1^2\,k_2^2} \ll \sum_{k_1,k_2\le x} k_1^{-\frac{3}{2}}\, k_2^{-\frac{3}{2}} \ll 1. \tag{300}$$

От (299) и (300) следва (298), с което лемата е доказана.

□

Ще използуваме също и следната проста

Лема 6.10. *При $x \ge 4$ е в сила оценката*

$$\sum_{n\le x} J(n) \gg \frac{x^2}{\log^2 x}. \tag{301}$$

Доказателство. От определението на $J(n)$ и от Теорема 5.4 (УАТЧ-1) следва

$$\sum_{n\le x} J(n) = \sum_{\substack{p_1,p_2\\ p_1+p_2\le x}} 1 \ge \sum_{p_1,p_2\le \frac{x}{2}} 1 = \pi^2\left(\frac{x}{2}\right) \gg \frac{x^2}{\log^2 x}.$$

□

От Леми 6.9 и 6.10 получаваме

Лема 6.11. *Нека $\mathcal{Q}$ е множеството, състоящо се числата 0, 1 и от естествените числа, представими като сума от две прости числа. Тогава за плътността му на Шнирелман имаме $d(\mathcal{Q}) > 0$.*

Доказателство. За произволно $n \in \mathbb{N}$ определяме

$$D(n) = \#\{k \in \mathcal{Q} \ : \ 1 \leq k \leq n\},$$

$$E(n) = \#\{k \in \mathbb{N} \ : \ 1 \leq k \leq n, \ J(k) > 0\}.$$

Очевидно

$$D(n) = 1 + E(n) \tag{302}$$

и в частност

$$D(1) = D(2) = D(3) = 1. \tag{303}$$

Нека $n \in \mathbb{N}$, $n \geq 4$. Прилагаме неравенството на Коши и получаваме

$$\left(\sum_{k \leq n} J(k)\right)^2 = \left(\sum_{\substack{k \leq n \\ J(k)>0}} J(k)\right)^2 \leq E(n) \sum_{k \leq n} J^2(k). \tag{304}$$

От Лема 6.9 знаем, че съществува константа $\alpha > 0$ такава, че

$$\sum_{k \leq n} J^2(k) \leq \alpha \frac{n^3}{\log^4 n}. \tag{305}$$

Съответно, от Лема 6.10 следва, че

$$\sum_{k \leq n} J(k) \geq \beta \frac{n^2}{\log^2 n}, \tag{306}$$

където $\beta > 0$ е константа. Тогава, като използуваме (304) – (306) виждаме, че при $n \geq 4$ е изпълнено

$$E(n) \geq \frac{\left(\sum_{k \leq n} J(k)\right)^2}{\sum_{k \leq n} J^2(k)} \geq \frac{\left(\beta \frac{n^2}{\log^2 n}\right)^2}{\alpha \frac{n^3}{\log^4 n}} = \beta^2 \alpha^{-1} n. \tag{307}$$

От (302), (303) и (307) следва, че

$$D(n) \geq \gamma n \qquad \text{за всяко} \qquad n \in \mathbb{N}.$$

където $\gamma > 0$ е константа. Тогава, според Определение 6.1, множеството $\mathcal{Q}$ има положителна плътност.

□

6.2.3 Доказателство на Теорема 6.8

Да вземем произволно $N \in \mathbb{N}$, $N > 1$. Тъй като числата 2 и 3 са прости, можем да считаме, че $N \geq 4$.

От Лема 6.7 и Лема 6.11 следва, че съществува константа s_0 такава, че всяко естествено число се представя като сума на най-много s_0 на брой числа от множеството $\mathcal{Q}$, определено в Лема 6.11. Тогава числото $N-2$ е сума на не повече от s_0 събираеми, всяко от които е равно на 1, или пък е сума на две прости числа. Следователно

$$N - 2 = m + M,$$

където $0 \leq m \leq s_0$, а за M знаем, че е сума на не повече от $2s_0$ на брой прости числа.

Ако $m = 0$, то $N = 2 + M$, следователно N е сума на не повече от $2s_0 + 1$ прости числа.

Ако $m = 1$, то $N = 3 + M$, следователно N отново е сума на не повече от $2s_0 + 1$ прости числа.

Да разгледаме сега случая $2 \leq m \leq s_0$. Ако m е четно, то се представя като сума на $\frac{m}{2} \leq s_0$ прости числа, всяко от които е равно на 2. Тогава числото $N = 2 + m + M$ е сума на не повече от $3s_0 + 1$ прости числа

Ако пък m е нечетно, то се представя като сума на $1 + \frac{m-3}{2} \leq s_0$ прости числа, първото от които е равно на 3, а останалите на 2. Тогава $N = 2 + m + M$ е отново сума на не повече от $3s_0 + 1$ прости числа.

Тогава, ако положим $k_0 = 3s_0 + 1$, виждаме, че всяко естествено $N > 1$ е сума на не повече от k_0 на брой прости числа, с което теоремата е доказана.

□

6.3 Приложение на метода на Шнирелман за решаване на проблема на Варинг

6.3.1 Формулировка на основните теореми

В настоящата глава ще разгледаме проблема на Варинг, който представлява обобщение на теоремата на Лагранж за представимостта на числата като сума от четири квадрата (виж (УАТЧ-1), глава). Ще докажем следната

Теорема 6.12. *За произволно $n \in \mathbb{N}$, $n \geq 2$ съществува $k = k(n) \in \mathbb{N}$ такова, че всяко естествено число се представя като сума на не повече от k на брой n-ти степени на естествени числа, т.е. за всяко $N \in \mathbb{N}$ диофантовото уравнение*

$$m_1^n + \cdots + m_k^n = N \tag{308}$$

с неизвестни $m_1, \ldots, m_k \in \mathbb{N}_0$ е разрешимо.

Въпросът за представимостта на числата като суми от степени е поставен от Варинг през 1770 г. През 18-ти и 19-ти век тази задача е решена само в някои частни случаи. Пълно решение е намерено от Хилберт през 1909 г., но неговото доказателство е изключително сложно. През 20-те години на 20-ти век Харди и Литлууд разработват така наречения „кръгов метод" и намират много по-просто решение на проблема на Варинг, като освен това дават явна формула за величината $k(n)$. По-късно И.Виноградов усъвършенства метода на Харди и Литлууд и значително подобрява оценката за $k(n)$. По-подробна информация за кръговия метод и неговите приложения може да бъде намерена в монографиите на Виноградов [2], Карацуба [4], Натансон [19], Вон [22], както и в записките на автора [6].

Да отбележим, че ако $k \leq n$, то числата, които могат да се представят като сума на k на брой n-ти степени, са разположени твърде рядко върху числовата ос, така че ще има безбройно много естествени числа непредставими в този вид. (При $k < n$ това е очевидно, а при $k = n$ кратко обяснение е дадено в началото на глава 11 на [4]). Поради това оттук нататък ще считаме, че е изпълнено

$$k \geq n + 1. \tag{309}$$

Предполага се, че ако е налице горното условие, то уравнението (308) е разрешимо за достатъчно големи стойности на N. Тази хипотеза не е доказана, но са получени резултати близки до нея. Повече информация по въпроса може да бъде намерена в монографиите, цитирани по-горе.

През 30-те години на 20-ти век Хуа-ло-Кен показва, че методът на Шнирелман, който изложихме в предишната глава, може да се използува и за решаване на проблема на Варинг. В настоящата глава ще приведем такова доказателство, като следваме изложението в монографиите на Гельфонд и Линник [5] и Натансон [19], но тук всички изчисления ще бъдат направени по-подробно.

Ще отбележим, че методът на Шнирелман позволява да бъде намерена явна формула за величината $k = k(n)$, но изразът който се получава представлява много бързо растяща функция на n. Тук ще установим само съществуването на $k(n)$ с описаното свойство, но формула няма да извеждаме.

Да пристъпим към решаването на проблема на Варинг с помощта на метода на Шнирелман. За целта разглеждаме множеството

$$\mathcal{A}_n = \{0, 1^n, 2^n, 3^n, 4^n, \dots\} \tag{310}$$

и определяме

$$\mathcal{B}_n^{(k)} = \underbrace{\mathcal{A}_n + \dots + \mathcal{A}_n}_{k \text{ пъти}}. \tag{311}$$

От Лема 6.7 и от определението на множеството $\mathcal{B}_n^{(k)}$ следва, че Теорема 6.12 е еквивалентна на следната

Теорема 6.13. *За всяко $n \in \mathbb{N}$, $n \geq 2$ съществува $k = k(n) \in \mathbb{N}$ такова, че плътността на Шнирелман на множеството $\mathcal{B}_n^{(k)}$ е положителна.*

На свой ред, Теорема 6.13 може да се получи като следствие от резултат, отнасящ се до средната стойност на експоненциалната сума

$$V_n(P;\alpha) = \sum_{0\le m\le P} e(\alpha m^n), \tag{312}$$

където $P \ge 1$ и α са реални параметри и, както обикновено, означаваме $e(t) = e^{2\pi it}$. При $k, n \in \mathbb{N}$, $P \in \mathbb{R}$, $P \ge 1$ определяме

$$I_{k,n}(P) = \int_0^1 |V_n(P;\alpha)|^{2k}\, d\alpha. \tag{313}$$

В сила е следната

Лема 6.14. *Величината $I_{k,n}(P)$ е равна на броя на решенията на уравнението*

$$m_1^n + \cdots + m_k^n = m_{k+1}^n + \cdots + m_{2k}^n \tag{314}$$

в неотрицателни цели числа $m_1, \ldots, m_{2k} \le P$.

Доказателство. Използуваме, че за всяко $z \in \mathbb{C}$ е изпълнено $|z|^2 = z\overline{z}$. Тогава от (312) и (313) следва

$$I_{k,n}(P) = \int_0^1 V_n(P;\alpha)^k\, \overline{V_n(P;\alpha)^k}\, d\alpha$$

$$= \int_0^1 \sum_{0\le m_1,\ldots,m_{2k}\le P} e\left(\alpha\left(m_1^n + \cdots + m_k^n - m_{k+1}^n - \cdots - m_{2k}^n\right)\right) d\alpha$$

$$= \sum_{0\le m_1,\ldots,m_{2k}\le P} \int_0^1 e\left(\alpha\left(m_1^n + \cdots + m_k^n - m_{k+1}^n - \cdots - m_{2k}^n\right)\right) d\alpha.$$

Но, според Лема 4.9 (5) (УАТЧ-1), интегралът в последния ред на горната формула е равен на 1, ако е в сила равенството (314), и на 0 в противен случай. С това лемата е доказана.

□

Сега ще видим, че ако разполагаме с достатъчно добра оценка отгоре за $I_{k,n}(P)$, то сме в състояние да докажем Теорема 6.13, а оттам и Теорема 6.12. По-точно, изпълнена е следната

Лема 6.15. *Нека $k, n \in \mathbb{N}$, $n \ge 2$, $k \ge n+1$, $P \in \mathbb{R}$, $P \ge 1$. Да допуснем, че е изпълнено неравенството*

$$I_{k,n}(P) \le \beta P^{2k-n} \qquad \text{за някое} \qquad \beta = \beta(k,n) > 0. \tag{315}$$

Тогава множеството $\mathcal{B}_n^{(k)}$, определено чрез (311)*, притежава положителна плътност, зависеща от k и n.*

Доказателство. За произволно $h \in \mathbb{N}_0$ означаваме

$$R(h) = R_{k,n}(h) = \#\{\langle m_1, \dots m_k\rangle \in {\mathbb{N}_0}^k \ : \ m_1^n + \cdots + m_k^n = h\} \tag{316}$$

и нека при $x \geq 1$ определим

$$U(x) = U_{k,n}(x) = \sum_{1 \leq h \leq x} R(h), \tag{317}$$

$$T(x) = T_{k,n}(x) = \sum_{1 \leq h \leq x} R^2(h). \tag{318}$$

Първо ще установим, че съществува $\alpha = \alpha(k,n) > 0$ такова, че

$$U(x) \geq \alpha x^{\frac{k}{n}} \qquad \text{за всяко} \qquad x \geq 1. \tag{319}$$

Да допуснем първо, че $1 \leq x \leq k$. Тогава, ако $1 \leq h \leq x$ имаме $R(h) \geq 1$, тъй като уравнението

$$m_1^n + \cdots + m_k^n = h$$

притежава решение

$$m_1 = \cdots = m_h = 1, \qquad m_{h+1} = \cdots = m_k = 0.$$

Тогава, като използуваме (309) и (317), получаваме

$$U(x) \geq [x] \geq \frac{1}{2}x \geq \frac{1}{2}k^{1-\frac{k}{n}}\, x^{\frac{k}{n}} \qquad \text{при} \qquad 1 \leq x \leq k. \tag{320}$$

Сега да разгледаме случая $k < x \leq 2k$. Тогава имаме

$$U(x) \geq \sum_{1 \leq h \leq k} R(h) \geq k \geq \frac{1}{2}x \geq \frac{1}{2}(2k)^{1-\frac{k}{n}}\, x^{\frac{k}{n}} \qquad \text{при} \qquad k < x \leq 2k. \tag{321}$$

Да разгледаме накрая случая $x > 2k$. Определяме

$$U'(x) = U(x) + 1 = \sum_{0 \leq h \leq x} R(h). \tag{322}$$

От (316) и (322) следва, че тази величина е равна на броя на решенията на неравенството

$$m_1^n + \cdots + m_k^n \leq x \tag{323}$$

в неизвестни $m_1, \dots, m_k \in \mathbb{N}_0$. Тъй като (323) се удовлетворява при

$$0 \leq m_j \leq \sqrt[n]{xk^{-1}}, \qquad 1 \leq j \leq k,$$

то имаме

$$U'(x) \geq \left(1 + \left[\sqrt[n]{xk^{-1}}\right]\right)^k \geq \left(xk^{-1}\right)^{\frac{k}{n}}. \tag{324}$$

От (309), (322) и (324) получаваме

$$U(x) \geq \left(xk^{-1}\right)^{\frac{k}{n}} - 1 \geq \frac{1}{2}k^{-\frac{k}{n}}\, x^{\frac{k}{n}} \qquad \text{при} \qquad x > 2k. \tag{325}$$

От (320), (321) и (325) следва (319) при, например, $\alpha = \frac{1}{2}(2k)^{-\frac{k}{n}}$.

Сега ще докажем, че съществува $\beta = \beta(k,n) > 0$ такова, че

$$T(x) \leq \beta x^{\frac{2k}{n}-1} \qquad \text{за всяко} \qquad x \geq 1. \tag{326}$$

За тази цел първо забелязваме, че от (316) следва, че $R^2(h)$ е равно на броя на $2k$-торките цели неотрицателни числа $m_1, \ldots, m_{2k}$ такива, че

$$m_1^n + \cdots + m_k^n = m_{k+1}^n + \cdots + m_{2k}^n = h.$$

Тогава, като използуваме (318) виждаме, че $T(x)$ не надхвърля броя на $2k$-торките цели неотрицателни числа $m_1, \ldots, m_{2k}$, удовлетворяващи

$$m_1^n + \cdots + m_k^n = m_{k+1}^n + \cdots + m_{2k}^n \leq x.$$

Но, ако последното условие е налице, то ще имаме

$$m_j \leq \sqrt[n]{x} \qquad \text{при} \qquad 1 \leq j \leq 2k.$$

Следователно, като приложим Лема 6.14 при $P = \sqrt[n]{x}$, получаваме

$$T(x) \leq I_{k,n}\left(\sqrt[n]{x}\,\right).$$

Сега използуваме условието (315) и получаваме, че е изпълнено неравенството (326), като β е величината, участваща в (315).

Да вземем произволно $x \geq 1$ и да означим с $D(x)$ броя на естествените числа $h \leq x$, за които $R(h) > 0$, или, все едно, които могат да се представят като сума от k на брой n-ти степени на цели неотрицателни числа. От (317), (318) и от неравенството на Коши следва, че

$$U(x) = \sum_{\substack{1 \leq h \leq x \\ R(h) > 0}} R(h) \leq \sqrt{D(x)\, T(x)}.$$

От последното неравенство и от (319), (326) получаваме

$$D(x) \geq \frac{U(x)^2}{T(x)} \geq \frac{\left(\alpha x^{\frac{k}{n}}\right)^2}{\beta x^{\frac{2k}{n}-1}} = \frac{\alpha^2}{\beta} x.$$

Тогава

$$\inf_{x \geq 1} \frac{D(x)}{x} \geq \frac{\alpha^2}{\beta} > 0,$$

следователно, според Определение 6.1, множеството $\mathcal{B}_n^{(k)}$ притежава положителна плътност, която зависи от k и n.

□

И така, виждаме, че за да докажем Теорема 6.12 е достатъчно да установим, че за всяко $n \in \mathbb{N}$, $n \geq 2$, може да се намери $k = k(n) \in \mathbb{N}$, така че да е в сила оценка от вида (315). Това е основната трудност, която трябва да преодолеем и с тази задача ще се занимаваме до края на настоящата глава.

Както ще видим по-долу, нужната оценка (315) за $I_{k,n}(P)$ може да бъде получена при

$$k = k(n) = \frac{1}{2} 8^{n-1}. \tag{327}$$

За да установим тази оценка при по-горе зададеното $k(n)$ ще използуваме индукция по n, но няма да доказваме директно (315), а по-общо твърдение. По-точно, вместо сумата $V_n(P; \alpha)$, зададена чрез (312) ще разглеждаме сумата

$$W(P; f, \alpha) = \sum_{0 \leq m \leq P} e\left(\alpha f(m)\right), \tag{328}$$

където

$$f(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_n \tag{329}$$

е полином с цели коефициенти, а вместо интеграла $I_{k,n}(P)$, определен чрез (313), ще оценяваме интеграла

$$J_{k,f}(P) = \int_0^1 |W(P; f; \alpha)|^{2k} \, d\alpha. \tag{330}$$

Причината поради която се налага доказването на такъв по-общ резултат е, че в частния случай не е ясно как да се направи индукционната стъпка по n, докато в по-общия случай тя се извършва, макар и не толкова лесно.

В сила е следната

Теорема 6.16. *Нека $P \in \mathbb{R}$, $P \geq 1$, $n \in \mathbb{N}$, $n \geq 2$ и k се определя от* (327)*. Нека $f(x) \in \mathbb{Z}[x]$ се задава чрез* (329) *и коефициентите му удовлетворяват условията*

$$1 \leq |a_0| \leq c, \qquad |a_1| \leq cP, \qquad |a_2| \leq cP^2, \qquad \ldots, \qquad |a_{n-1}| \leq cP^{n-1}, \tag{331}$$

където $c = c(n, f) > 1$ не зависи от P. Тогава съществува $\beta = \beta(c, n, f) > 0$, не зависещо от P и такова, че за интеграла (330) *имаме*

$$J_{k,f}(P) \leq \beta \, P^{2k-n}. \tag{332}$$

От тази теорема получаваме, като частен случай

Теорема 6.17. *Нека $P \in \mathbb{R}$, $P \geq 1$, $n \in \mathbb{N}$, $n \geq 2$ и нека k се определя от* (327)*. Тогава съществува $\beta = \beta(n) > 0$, не зависещо от P и такова, че за интеграла* (313) *имаме*

$$I_{k,n}(P) \leq \beta \, P^{2k-n}. \tag{333}$$

И така, ако докажем Теорема 6.16, то от нейното следствие (Теорема 6.17) и от Лема 6.15 получаваме доказателство на Теорема 6.13, а от нея, както разбрахме, следва и доказателството на Теорема 6.12.

6.3.2 Някои леми

Ще започнем със следната

Лема 6.18. *Нека $h \in \mathbb{Z}$, $x, y \in \mathbb{R}$ и $x, y \geq 1$. Нека $q(h; x, y)$ означава броя на решенията на уравнението*

$$k_1 l_1 + k_2 l_2 = h \tag{334}$$

в цели числа k_1, k_2, l_1, l_2, удовлетворяващи условията

$$|k_1|, |k_2| \leq x, \qquad |l_1|, |l_2| \leq y. \tag{335}$$

В сила е оценката

$$q(h; x, y) \ll \begin{cases} xy \sum\limits_{d|h} \dfrac{1}{d} & \text{при} \quad h \neq 0, \\ \\ x^2 + y^2 + (xy)^{1+\varepsilon} & \text{при} \quad h = 0, \end{cases} \tag{336}$$

където $\varepsilon > 0$ е произволно малко и в случая $h = 0$ константата в знака $\ll$ зависи от ε.

Доказателство. Да разгледаме първо случая $h = 0$. Имаме

$$q(0; x, y) = q' + q'', \tag{337}$$

където q' е броят на решенията на уравнението

$$k_1 l_1 + k_2 l_2 = 0 \tag{338}$$

в цели числа удовлетворяващи (335) и такива, че $k_2 l_2 \neq 0$, и, съответно, q'' е броят на останалите решения (т.е. за които $k_2 l_2 = 0$).

Да оценим q'. Ако са изпълнени условията (335) и (338) и ако $k_2 l_2 \neq 0$, то очевидно имаме $k_1 l_1 \neq 0$. Тъй като числата k_1, l_1 могат да приемат не повече от, съответно, $2x$, $2y$ на брой стойности, а при фиксирани k_1, l_1 броят на допустимите двойки k_2, l_2 не надхвърля $2\tau(|k_1 l_1|)$, то като използуваме Лема 3.33 (УАТЧ-1), получаваме

$$q' \ll (xy)^{1+\varepsilon}, \tag{339}$$

където $\varepsilon > 0$ е произволно малко.

Сега да разгледаме q''. Ако $k_2 l_2 = 0$, то някое от числата k_2, l_2 е равно на нула, следователно броят на допустимите двойки k_2, l_2 не надвърля $2x + 1 + 2y + 1 \ll x + y$. Имаме също $k_1 l_1 = 0$, откъдето следва, че броят на допустимите двойки k_1, l_1 също е $\ll x + y$. Тогава

$$q'' \ll (x + y)^2 \ll x^2 + y^2. \tag{340}$$

От (337), (339) и (340) следва оценката (336) в случая $h = 0$.

Сега да разгледаме случая $h \neq 0$. Без ограничение на общността можем да считаме, че

$$x \leq y. \tag{341}$$

От (334) следва, че поне едно от числата k_1, k_2 е различно от нула. Ако означим с $q_1(h; x, y)$ броя на решенията на (334) в цели числа, удовлетворяващи условията

$$1 \leq |k_1| \leq x, \qquad |k_2| \leq |k_1|, \qquad |l_1|, |l_2| \leq y, \tag{342}$$

то ще имаме

$$q(h; x, y) \leq 2q_1(h; x, y). \tag{343}$$

За да оценим $q_1(h; x, y)$ групираме решенията на (334), (342) съобразно стойността на най-големия общ делител на k_1 и k_2. Ако $(k_1, k_2) = d$, то ще имаме $d \mid h$ и ще съществуват $r_1, r_2 \in \mathbb{Z}$, за които $k_i = dr_i$, $i = 1, 2$. Тогава ще имаме

$$r_1 l_1 + r_2 l_2 = \frac{h}{d}, \qquad (r_1, r_2) = 1, \qquad |r_2| \leq |r_1| \leq \frac{x}{d},$$

откъдето

$$q_1(h; x, y) = \sum_{d \mid h} q_2\left(\frac{h}{d}; \frac{x}{d}, y\right), \tag{344}$$

а $q_2(s; z, y)$ означава броя на решенията на

$$r_1 l_1 + r_2 l_2 = s \tag{345}$$

в цели числа r_1, r_2, l_1, l_2, удовлетворяващи условията

$$(r_1, r_2) = 1, \qquad 1 \leq |r_1| \leq z, \qquad |r_2| \leq |r_1|, \qquad |l_1|, |l_2| \leq y.$$

За да оценим величината $q_2(s; z, y)$ при

$$s \neq 0, \qquad 1 \leq z \leq x \tag{346}$$

използуваме равенството

$$q_2(s; z, y) = \sum_{1 \leq |r_1| \leq z} \sum_{\substack{|r_2| \leq |r_1| \\ (r_1, r_2) = 1}} q_3(s; r_1, r_2, y), \tag{347}$$

където $q_3(s; r_1, r_2, y)$ означава броя на решенията на (345) в променливи $l_1, l_2 \in \mathbb{Z}$, удовлетворяващи

$$|l_1|, |l_2| \leq y. \tag{348}$$

Нека l_1', l_2' е фиксирано решение на (345), (348). Тогава всичките решения на (345) се задават чрез формулите

$$l_1 = l_1' + tr_2, \qquad l_2 = l_2' - tr_1, \tag{349}$$

където $t \in \mathbb{Z}$. Наистина, ако l_1, l_2 е някакво решение, то имаме

$$r_1(l_1 - l_1') + r_2(l_2 - l_2') = 0$$

и тъй като $r_1 \neq 0$ и $(r_1, r_2) = 1$, то получаваме $r_1 \mid l_2 - l_2'$, т.е. $l_2 - l_2' = -r_1 t$ за някое $t \in \mathbb{Z}$. Като заместим в горното уравнение и разделим на r_1 получаваме и $l_1 - l_1' = r_2 t$.

Поради горните съображения величината $q_3(s; r_1, r_2, y)$ не надминава броя на целите числа t, за които числата l_1, l_2, определени от (349), удовлетворяват (348). Тъй като $t = \frac{l_2' - l_2}{r_1}$, имаме

$$|t| \leq \frac{|l_2'| + |l_2|}{|r_1|} \leq \frac{2y}{|r_1|},$$

откъдето

$$q_3(s; r_1, r_2, y) \leq \frac{4y}{|r_1|} + 1.$$

Заместваме в (347) и, като вземем предвид (341) и (346), получаваме

$$\begin{aligned} q_2(s; z, y) &\leq \sum_{1 \leq |r_1| \leq z} \sum_{|r_2| \leq |r_1|} \left(\frac{4y}{|r_1|} + 1 \right) \\ &= \sum_{1 \leq |r_1| \leq z} \left(\frac{4y}{|r_1|} + 1 \right) (2|r_1| + 1) \\ &\leq 15 \sum_{1 \leq |r_1| \leq z} y \\ &\leq 30zy. \end{aligned}$$

От горната оценка и от (343), (344) получаваме

$$q(h; x, y) \ll \sum_{d \mid h} \frac{x}{d} y = xy \sum_{d \mid h} \frac{1}{d},$$

с което лемата е доказана.

□

Следващата лема представлява вариант на Лема 6.18 в случая $h = 0$.

Лема 6.19. *Нека $x, y \in \mathbb{R}$ и*

$$1 \leq x \leq y. \tag{350}$$

Означаваме с $q^*(x, y)$ броя на решенията на уравнението

$$k_1 l_1 + k_2 l_2 = 0 \tag{351}$$

в цели числа k_1, k_1, l_1, l_2, удовлетворяващи условията

$$1 \leq |k_1|, |k_2| \leq x, \qquad |l_1|, |l_2| \leq y. \tag{352}$$

В сила е оценката

$$q^*(x, y) \ll (xy)^{1+\varepsilon}, \tag{353}$$

където $\varepsilon > 0$ е произволно малко и константата в знака $\ll$ зависи само от ε.

Доказателство. Ясно е, че

$$q^*(x,y) = q' + q_0,$$

където q' е броят на решенията на (351), (352) за които $l_1 l_2 \neq 0$, а q_0 е броят на решенията, за които $l_1 = l_2 = 0$. Величината q' оценихме в началото на доказателството на Лема 6.18 и установихме неравенството (339). Очевидно е също, че $q_0 \ll x^2$ и, като използуваме (350), получаваме (353).

□

Сега ще се занимаем с изследване на броя на решенията на уравнението

$$k_1 l_1 + k_2 l_2 = k_3 l_3 + k_4 l_4 \tag{354}$$

в променливи, намиращи се в определени области.

Ще започнем със следната

Лема 6.20. *Нека $x, y \in \mathbb{R}$, $x, y \geq 1$. Означаваме с $T(x,y)$ броя на решенията на уравнението* (354) *в цели числа $k_1, \ldots, k_4, l_1, \ldots, l_4$, удовлетворяващи*

$$|k_1|, \ldots, |k_4| \leq x, \qquad |l_1|, \ldots, |l_4| \leq y. \tag{355}$$

Тогава е в сила оценката

$$T(x,y) \ll x^3 y^3 + x^4 + y^4. \tag{356}$$

като константата в знака $\ll$ е абсолютна.

Доказателство. Имаме

$$T(x,y) = \sum_{|h| \leq 2xy} F(h;x,y),$$

където $F(h;x,y)$ означава броя на решенията на системата от две уравнения

$$k_1 l_1 + k_2 l_2 = k_3 l_3 + k_4 l_4 = h$$

в цели числа $k_1, \ldots, k_4, l_1, \ldots, l_4$, удовлетворяващи (355). Ясно е, че

$$F(h;x,y) = q^2(h;x,y), \tag{357}$$

където $q(h;x,y)$ е величината, определена в Лема 6.18. Тогава имаме

$$T(x,y) = T_1 + T_2, \tag{358}$$

където

$$T_1 = q^2(0;x,y), \qquad T_2 = \sum_{1 \leq |h| \leq 2xy} q^2(h;x,y).$$

От оценката (336) в случая $h = 0$, която е дадена в Лема 6.18, непосредствено следва, че

$$T_1 \ll x^4 + y^4 + x^3y^3. \tag{359}$$

Да разгледаме сега T_2. От оценката (336) в случая $h \neq 0$ получаваме

$$T_2 \ll \sum_{1\leq|h|\leq 2xy} \left(xy \sum_{d|h} \frac{1}{d} \right)^2 \ll x^2y^2\, T_3, \tag{360}$$

където

$$T_3 = \sum_{1\leq h\leq 2xy} \left(\sum_{d|h} \frac{1}{d} \right)^2 = \sum_{1\leq h\leq 2xy} \sum_{\substack{d_1|h \\ d_2|h}} \frac{1}{d_1 d_2}.$$

Сега, като сменим реда на сумиране и използуваме определението за най-малко общо кратно на две числа, виждаме, че

$$T_3 = \sum_{d_1,d_2\leq 2xy} \frac{1}{d_1 d_2} \sum_{\substack{h\leq 2xy \\ h\equiv 0 \pmod{d_1} \\ h\equiv 0 \pmod{d_2}}} 1$$

$$= \sum_{d_1,d_2\leq 2xy} \frac{1}{d_1 d_2} \sum_{\substack{h\leq 2xy \\ h\equiv 0 \pmod{[d_1,d_2]}}} 1$$

$$\ll \sum_{d_1,d_2\leq 2xy} \frac{1}{d_1 d_2} \cdot \frac{xy}{[d_1,d_2]}.$$

Тогава имаме

$$T_3 \ll xy\, \Sigma_0, \qquad \Sigma_0 = \sum_{d_1,d_2\leq 2xy} \frac{1}{d_1\, d_2\, [d_1,d_2]}. \tag{361}$$

Величината Σ_0 е подобна на сумата F_1, определена чрез (299), и за която получихме оценката (300). По същия начин виждаме, че $\Sigma_0 \ll 1$ и, като заместим в (361) получаваме

$$T_3 \ll xy.$$

От горната оценка и от (360) следва

$$T_2 \ll x^3y^3. \tag{362}$$

Прилагаме (358), (359) и (362) и получаваме (356), с което лемата е доказана.

□

Накрая, ще изведем и следния вариант на Лема 6.20. Имаме

Лема 6.21. *Нека $x, y \in \mathbb{R}$, $1 \leq x \leq y$. Означаваме с $T^*(x,y)$ броя на решенията на уравнението* (354) *в цели числа $k_1, \ldots, k_4, l_1, \ldots, l_4$, удовлетворяващи*

$$1 \leq |k_1|, \ldots, |k_4| \leq x, \qquad |l_1|, \ldots, |l_4| \leq y. \tag{363}$$

Тогава е в сила оценката

$$T^*(x,y) \ll x^3 y^3, \tag{364}$$

като константата в знака $\ll$ е абсолютна.

Доказателство. Разсъждаваме както в доказателството на Лема 6.20, но вместо оценката (336) за величината $q(0;x,y)$, получена в Лема 6.18, прилагаме оценката за $q^*(x,y)$, дадена в Лема 6.19. Проверката оставяме на читателя.

□

6.3.3 Доказателство на Теорема 6.16

Ще докажем твърдението с индукция по n. Да разгледаме случая $n = 2$. Тогава от (327) следва, че $k = 4$. Нека

$$f(x) = a_0 x^2 + a_1 x + a_2 \tag{365}$$

е полином с цели коефициенти, удовлетворяващи

$$1 \leq |a_0| \leq c, \qquad |a_1| \leq cP. \tag{366}$$

където $c > 1$ е константа. Разглеждаме сумата

$$W(P; f, \alpha) = \sum_{0 \leq m \leq P} e(\alpha f(m)). \tag{367}$$

Ще установим, че за интеграла

$$J = \int_0^1 |W(P; f, \alpha)|^8 \, d\alpha \tag{368}$$

е изпълнено

$$J \leq \beta P^6 \tag{369}$$

за някое $\beta > 0$, което не зависи от P.

Имаме

$$J = \int_0^1 W(P; f, \alpha)^4 \, W(P; f, -\alpha)^4 \, d\alpha = \int_0^1 \sum_{0 \leq m_1, \ldots, m_8 \leq P} e(\alpha F(m_1, \ldots, m_8)) \, d\alpha. \tag{370}$$

където

$$F = F(m_1, \ldots, m_8) = \sum_{i=1}^{4} (f(m_i) - f(m_{i+4})) \tag{371}$$

В последния израз от формула (370) сменяме реда на сумирането и интегрирането и, като използуваме Лема 4.9 (5) (УАТЧ-1), получаваме че интегралът J е равен на броя на решенията на уравнението

$$F = 0 \tag{372}$$

в променливи $m_1, \ldots, m_8 \in \mathbb{Z}$, удовлетворяващи условията

$$0 \leq m_1, \ldots, m_8 \leq P. \tag{373}$$

От (365) и (371) получаваме

$$F = \sum_{i=1}^{4} \big(a_0(m_i^2 - m_{i+4}^2) + a_1(m_i - m_{i+4})\big) = \sum_{i=1}^{4} u_i v_i,$$

където

$$u_i = m_i - m_{i+4}, \qquad v_i = a_0(m_i + m_{i+4}) + a_1, \qquad 1 \leq i \leq 4. \tag{374}$$

От (366), (373) и (374) следва, че

$$|u_i|, |v_i| \leq c'P, \qquad 1 \leq i \leq 4, \tag{375}$$

където $c' > 1$ е константа, зависеща само от c.

Ясно е, че при зададени u_i, v_i съществува най-много една двойка числа m_i, m_{i+4}, за които е изпълнено (374). Тогава, ако означим с J' броя на решенията на уравнението

$$\sum_{i=1}^{4} u_i v_i = 0$$

в цели числа u_i, v_i, за които е изпълнено (375). то имаме

$$J \leq J'. \tag{376}$$

Очевидно е, че J' е равно също и на броя на решенията на

$$u_1 v_1 + u_2 v_2 = u_3 v_3 + u_4 v_4$$

в цели числа, удовлетворяващи (375). Тогава, като приложим Лема 6.20, получаваме

$$J' \ll P^6.$$

От последната оценка и от (376) следва (369).

Да допуснем, че твърдението на Теорема 6.16 е изпълнено за някое $n \geq 2$. Нашата цел е да докажем, че твърдението е вярно и за $n+1$. Нека е даден полином от $n+1$-ва степен

$$f(x) = a_0 x^{n+1} + a_1 x^n + \cdots + a_{n+1} \tag{377}$$

с цели коефициенти, удовлетворяващи

$$1 \le |a_0| \le c, \qquad |a_1| \le cP, \qquad |a_2| \le cP^2, \qquad \dots, \qquad |a_n| \le cP^n, \tag{378}$$

където $c = c(n, f) > 1$ не зависи от P. Ще установим, че за сумата

$$W(P; f, \alpha) = \sum_{0 \le m \le P} e(\alpha f(m)) \tag{379}$$

е в сила оценката

$$\int_0^1 |W(P; f, \alpha)|^{8^n} \, d\alpha \ll P^{8^n - (n+1)}. \tag{380}$$

Като използуваме (379) виждаме, че

$$|W(P; f, \alpha)|^2 = W(P; f, \alpha)\, W(P; f, -\alpha) = \sum_{0 \le m \le P} \sum_{0 \le m_1 \le P} e(\alpha(f(m_1) - f(m))).$$

Във вътрешната сума извършваме смяна на променливата $m_1 = m + h$, след което сменяме реда на сумиране и получаваме

$$|W(P; f, \alpha)|^2 = \sum_{0 \le m \le P} \sum_{-m \le h \le P - m} e(\alpha(f(m+h) - f(m))).$$

$$= \sum_{|h| \le P} \sum_{m \in I_h} e(\alpha(f(m+h) - f(m))), \tag{381}$$

където

$$I_h = [0, P] \cap [-h, P - h]. \tag{382}$$

Очевидно е, че вътрешната сума в (381) по модул не надхвърля $P + 1$. Тогава, ако при $h \ne 0$ положим

$$g_h(x) = \frac{f(x+h) - f(x)}{h} \tag{383}$$

и

$$Z(\alpha, h) = \sum_{m \in I_h} e\left(\alpha h\, g_h(m)\right), \tag{384}$$

то, като използуваме (381), виждаме, че

$$|W(P; f, \alpha)|^2 \le 2P + \sum_{1 \le |h| \le P} |Z(\alpha, h)|. \tag{385}$$

Да отбележим, че от (377) и (383) следва, че полиномът $g_h(x)$ се представя във вида

$$g_h(x) = B_0 x^n + B_1 x^{n-1} + \dots + B_n \in \mathbb{Z}[x], \tag{386}$$

където

$$B_i = \sum_{\nu=0}^{i} \binom{n+1-\nu}{i+1-\nu} a_\nu h^{i-\nu}, \qquad 0 \le i \le n.$$

От горната формула и от условията (378) следва, че съществува $c^* > 1$, не зависещо от P и такова, че при $0 < |h| \le P$ имаме

$$1 \le |B_0| \le c^*, \qquad |B_1| \le c^* P, \qquad |B_2| \le c^* P^2, \qquad \ldots, \qquad |B_n| \le c^* P^n. \tag{387}$$

От (386) и (387) се вижда също, че за някое $\gamma_0 > 1$, което не зависи от P, имаме

$$|g_h(x)| \le \gamma_0 P^n \qquad \text{при} \qquad 0 \le x \le P, \qquad |h| \le P. \tag{388}$$

Да положим, за простота на записа,

$$t = \frac{1}{2} 8^{n-1} \tag{389}$$

Повдигаме двете страни на (385) в степен $2t$ и, като използуваме неравенството на Хьолдер, получаваме

$$|W(P; f, \alpha)|^{4t} \ll P^{2t} + \left(\sum_{1 \le |h| \le P} |Z(\alpha, h)| \right)^{2t}$$

$$\ll P^{2t} + P^{2t-1} \sum_{1 \le |h| \le P} |Z(\alpha, h)|^{2t}, \tag{390}$$

като константата в знака $\ll$ зависи само от n. Сега използуваме (384) и намираме, че

$$|Z(\alpha, h)|^{2t} = Z(\alpha, h)^t Z(-\alpha, h)^t = \sum_{m_1, r_1, \ldots, m_t, r_t \in I_h} e\left(\alpha h\, G_h(m_1, r_1, \ldots, m_t, r_t)\right), \tag{391}$$

където

$$G = G_h(m_1, r_1, \ldots, m_t, r_t) = g_h(m_1) + \cdots + g_h(m_t) - g_h(r_1) - \cdots - g_h(r_t). \tag{392}$$

Разделяме сумата от дясната страна на (391) на части съобразно стойността на величината G, зададена чрез (392). Нека $A_h(s)$ означава броя на решенията на уравнението

$$G_h(m_1, r_1, \ldots, m_t, r_t) = s$$

в цели числа $m_1, r_1, \ldots, m_t, r_t \in I_h$. Използуваме също (388) и виждаме, че за някое $\gamma > 1$, което не зависи от P, имаме

$$|Z(\alpha, h)|^{2t} = \sum_{|s| \le \gamma P^n} A_h(s)\, e(\alpha h s). \tag{393}$$

(Можем да вземем, например, $\gamma = 2t\gamma_0$, където γ_0 е константата от (388)). Като използуваме (384), определението на $A_h(s)$ и Лема 4.9 (5) (УАТЧ-1), намираме

$$A_h(s) = \sum_{m_1,r_1,\dots,m_t,r_t \in I_h} \int_0^1 e(\alpha(g_h(m_1) + \cdots + g_h(m_t) - g_h(r_1) - \cdots - g_h(r_t) - s))\, d\alpha$$

$$= \int_0^1 |Z(\alpha, h)|^{2t} e(-\alpha s)\, d\alpha.$$

Оттук получаваме

$$A_h(s) \leq \int_0^1 |Z(\alpha, h)|^{2t}\, d\alpha = A_h(0). \tag{394}$$

От (382) следва, че $I_h \subset [0, P]$ и, като си припомним определението за $A_h(0)$, виждаме, че

$$A_h(0) \leq A', \tag{395}$$

където A' означава броя на решенията на уравнението

$$g_h(m_1) + \cdots + g_h(m_t) - g_h(r_1) - \cdots - g_h(r_t) = 0$$

в променливи m_j, r_j, удовлетворяващи

$$0 \leq m_1, r_1, \dots, m_t, r_t \leq P.$$

Като се възползуваме отново от Лема 4.9 (5) (УАТЧ-1) виждаме, че

$$A' = \sum_{0 \leq m_1,r_1,\dots,m_t,r_t \leq P} \int_0^1 e(\alpha(g_h(m_1) + \cdots + g_h(m_t) - g_h(r_1) - \cdots - g_h(r_t)))\, d\alpha$$

$$= \int_0^1 |W^*(P; g_h, \alpha)|^{2t}\, d\alpha,$$

където

$$W^*(P; g_h, \alpha) = \sum_{0 \leq m \leq P} e(\alpha g_h(m)).$$

От (386), (387), (389) и от индукционното предположение следва

$$A' \ll P^{8^{n-1}-n}. \tag{396}$$

Тогава от неравенствата (394) – (396) виждаме, че

$$A_h(s) \ll P^{8^{n-1}-n} \qquad \text{при} \qquad |s| \leq \gamma P^n. \tag{397}$$

Повдигаме неравенството (390) в четвърта степен, използуваме (389), (393) и получаваме

$$|W(P;f,\alpha)|^{8^n} \ll P^{\frac{1}{2}8^n} + P^{\frac{1}{2}8^n-4}\,|U(\alpha)|^4,$$

където

$$U(\alpha) = \sum_{1\le|h|\le P}\ \sum_{|s|\le\gamma P^n} A_h(s)\,e(\alpha hs). \tag{398}$$

Оттук следва

$$\int_0^1 |W(P;f,\alpha)|^{8^n}\,d\alpha \ll P^{\frac{1}{2}8^n} + P^{\frac{1}{2}8^n-4}\int_0^1 |U(\alpha)|^4\,d\alpha. \tag{399}$$

Сега ще оценим интеграла от дясната страна на последното неравенство. Като използуваме (398), намираме

$$\begin{aligned}|U(\alpha)|^4 &= U(\alpha)^2\,U(-\alpha)^2\\ &= \sum_{h_j,s_j\ (400)} A_{h_1}(s_1)A_{h_2}(s_2)A_{h_3}(s_3)A_{h_4}(s_4)\\ &\qquad\times e(\alpha(h_1s_1+h_2s_2-h_3s_3-h_4s_4)),\end{aligned}$$

където сумирането се извършва по $h_j, s_j, 1\le j\le 4$, удовлетворяващи условията

$$1\le|h_1|,\dots,|h_4|\le P,\qquad |s_1|,\dots,|s_4|\le\gamma P^n. \tag{400}$$

Оттук и от Лема 4.9 (5) (УАТЧ-1) следва

$$\begin{aligned}\int_0^1 |U(\alpha)|^4\,d\alpha &= \sum_{h_j,s_j\ (400)} A_{h_1}(s_1)A_{h_2}(s_2)A_{h_3}(s_3)A_{h_4}(s_4)\\ &\qquad\times\int_0^1 e(\alpha(h_1s_1+h_2s_2-h_3s_3-h_4s_4))\,d\alpha\\ &= \sum_{h_j,s_j\ (400),\ (401)} A_{h_1}(s_1)A_{h_2}(s_2)A_{h_3}(s_3)A_{h_4}(s_4),\end{aligned}$$

като в последната формула сумирането се извършва по променливи, удовлетворяващи (400) и също уравнението

$$h_1s_1+h_2s_2-h_3s_3-h_4s_4=0. \tag{401}$$

Прилагаме (397) и получаваме

$$\int_0^1 |U(\alpha)|^4 \, d\alpha \ll P^{4\cdot 8^{n-1}-4n} \, \mathcal{F},$$

където $\mathcal{F}$ е броят на осморките цели числа $h_1, s_1, \ldots, h_4, s_4$, удовлетворяващи (400) и (401). Сега, като приложим Лема 6.21, получаваме

$$\mathcal{F} \ll P^{3n+3},$$

откъдето следва

$$\int_0^1 |U(\alpha)|^4 \, d\alpha \ll P^{4\cdot 8^{n-1}-n+3}.$$

От горното неравенство и от (399) получаваме

$$\int_0^1 |W(P, f, \alpha)|^{8^n} \, d\alpha \ll P^{\frac{1}{2}8^n} + P^{\frac{1}{2}8^n-4} \cdot P^{4\cdot 8^{n-1}-n+3} \ll P^{8^n-(n+1)}.$$

С това оценката (380) е доказана и доказателството на теоремата е завършено.

□

Литература

[1] И. М. Виноградов, *Основы теории чисел*, „Наука”, Москва, 1981.

[2] И. М. Виноградов, *Метод тригонометрических сумм в теории чисел*, „Наука”, Москва, 1971.

[3] И. М. Виноградов, *Представление нечетного числа суммой трех простых чисел*, ДАН СССР, 15, (1937), 6–7.

[4] А. А. Карацуба, *Основы аналитической теории чисел*, „Наука”, Москва, 1983.

[5] А. О. Гельфонд, Ю. В. Линник *Элементарные методы в аналитической теории чисел* „Физматгиз”, Москва, 1962.

[6] Д. И. Толев, *Адитивни задачи в теорията на числата*, Записки по едноименния изборен курс, четен във ФМИ през учебната 2008/2009 г. http://www.fmi.uni-sofia.bg/econtent/

[7] Д. И. Толев, *Увод в аналитичната теория на числата*, Записки по едноименния изборен курс, четен във ФМИ през учебната 2010/2011 г. http://www.fmi.uni-sofia.bg/econtent/

[8] Д. И. Толев, *Увод в аналитичната теория на числата II*, Записки по едноименния изборен курс, четен във ФМИ през учебната 2011/2012 г. http://www.fmi.uni-sofia.bg/econtent/

[9] T. Estermann, *Einige Sätze über quadratfeie Zahlen*, Math. Ann., 105, (1931), 653–662.

[10] D. Goldston, J. Pintz, C. Yildirim, *Primes in tuples I*, Ann. of Math. (2) 170 (2009), 2, 819-862.

[11] D. Goldston, J. Pintz, C. Yildirim, *Primes in tuples II*, Acta Math. 204 (2010), 1, 1-47.

[12] J. Friedlander, H. Iwaniec, *Opera de Cribro*, Amer. Math. Soc. Colloquium Publications, 57, 2010.

[13] H. Halberstam, H. E. Richert, *Sieve Methods*, Academic Press, London, 1974.

[14] D. R. Heath-Brown, *Square-free values of* $n^2 + 1$, Acta Arith. 155 (2012), 1–13.

[15] H. A. Helfgott, *Major arcs for Goldbach's problem*, arXiv:math.NT/1305.2897v2.

[16] H. A. Helfgott, *Minor arcs for Goldbach's problem*, arXiv:math.NT/1205.5252v3.

[17] L-K. Hua, *Introduction to Number Theory*, Springer, 1982.

[18] H. Iwaniec, E. Kowalski, *Analytic number theory*, Amer. Math. Soc. Colloquium Publications, 53, 2004.

[19] M. B. Nathanson, *Additive Number Theory: The Classical Bases*, Graduate Texts in Mathematics, 164, Springer, New York, 1996.

[20] J. Pintz, *A note on bounded gaps between primes*, arXiv:math.NT/1306.1479v2.

[21] D. I. Tolev, *On the number of pairs of positive integers* $x, y \leq H$ *such that* x^2+y^2+1 *is squarefree*, Monatsh. Math. 165 (2012), 557–567.

[22] R. C. Vaughan, *The Hardy-Littlewood Method*, Sec. ed, Cambridge Univ. Press, 1997.

[23] Y. Zhang, *Bounded gaps between primes*, Ann. of Math., to appear.