Увод в аналитичната теория на числата

Д. И. Толев

Записки по едноименния изборен курс, четен от автора
във ФМИ при СУ „Св. Климент Охридски“
през зимния семестър на учебната
2010/2011 г.

София, септември 2011 г.

Съдържание

1 Увод

В настоящите записки е изложен материала от изборния курс, четен от автора във Факултета по Математика и Информатика при Софийския Университет през зимния семестър на учебната 2010/2011 г. Целта е да бъдат запознати читателите с някои от основните понятия и теореми от елементарната и от аналитичната теория на числата.

Глава 2 е помощна. В нея са изложени прости леми от математическия анализ и са получени техни следствия, които по-късно се използуват често.

В Глава 3 са изложени определения и теореми, отнасящи се до делимостта на числата и сравненията. Въведени са основните аритметични функции и са изучени свойствата им. Накрая са изведени точните формули на Якоби за броя на представянията на числата като суми от два и от четири квадрата.

В Глава 4 се разглеждат проблемите на Гаус и на Дирихре, отнасящи се до намиране на приближени формули за броя на целите точки в кръга и, съответно, под хиперболата. Показано е как оценяването на остатъчните членове в тези формули се свежда до изследването на експоненциални суми и е доказана теоремата на Ван-дер-Корпут за оценка на такива суми. По такъв начин са доказани теоремите на Вороной за задачите на Гаус и Дирихле.

Глава 5 се извеждат класически теореми за разпределението на простите числа. Първо са формулирани и доказани теоремите на Чебишев и Мертенс и са получени техни следствия. След това са въведени дзета-функцията на Риман и L-функциите на Дирихле. Показано, че от техните аналитични свойства (най-вече, от отсъствието на нули в някои области от комплексната равнина) следват резултати, отнасящи се простите числа, а именно асимптотичния закон за разпределението на простите числа и теоремата на Дирихле за простите числа в аритметични прогресии.

При изготвянето на настоящите записки са използувани няколко добре известни книги, които са цитирани в литературата. Тук обаче доказателствата са изложени по-подробно и изчисленията са приведени почти навсякъде.

Авторът няма претенции, че записките представляват пълно и систематично въведение в елементарната и в аналитичната теория на числата. Не са споменати много от важните понятия и резултати — например символът на Льожандър и законът за реципрочност на квадратичните остатъци. Надявам се, че в следващите редакции тези празноти ще бъдат поне частично запълнени.

Накрая бих искал да изкажа благодарност на Артур Киркорян, Владимир Митанкин, Стефан Василев и Стоян Димитров за посочването на някои грешки и неточности, допуснати в първоначалния вариант на записките и също на Владимир Митанкин за изготвяне на чертежите.

Означения

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 считаме, че $i = \sqrt{-1}$. С буквата s ще означаваме комплексно число, като ще го записваме обикновено във вида $s = \sigma + i\tau$. Реалната част, имагинерната част и аргумента на s ще означаваме с $Re(s)$, $Im(s)$, $arg(s)$, а за комплексно спрегнатото число на s ще използуваме означението $\overline{s}$. Буквата ε ще използуваме за произволно малко положително число, което не е едно и също в различни формули.

Сума или произведение по естествените числа n, ненадминаващи величината x, ще означаваме накратко с $\sum_{n\le x}$, съответно $\prod_{n\le x}$. Аналогично, за сума или произведение по простите числа p, ненадминаващи x, ще използуваме означенията $\sum_{p\le x}$ и $\prod_{p\le x}$. Сума и произведение по всички прости числа ще означаваме с $\sum_p$ и съответно $\prod_p$. Ако $n \in \mathbb{N}$, то $\sum_{d|n}$ означава сума, в която сумирането се извършва по всички положителни делители на n. Съответно $\sum_{p|n}$ означава сума по простите делители на n.

С буквата γ ще бележим константата на Ойлер. Тя се определя чрез равенството

$$\gamma = \lim_{N\to\infty}\left(\sum_{n=1}^{N}\frac{1}{n} - \log N\right), \tag{1}$$

С $\log x$ ще означаваме натурален логаритъм на x. Както обикновено, $[x]$ ще бъде цялата част на x, т.е. най-голямото цяло число, ненадминаващо x,

$$\{x\} = x - [x] \tag{2}$$

ще бъде дробната част на x и $||x||$ ще бъде разстоянието от x до най-близкото цяло число. Ще означаваме също

$$e(x) = e^{2\pi i x}. \tag{3}$$

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

$$f(x) \sim g(x) \qquad \text{при} \qquad x \to \infty.$$

По аналогичен начин се определя асимптотично равенство между две функции, когато аргументът им 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 $|X| \leq cY$“. Ако c зависи от някои други константи, например γ, δ то понякога ще отразяваме този факт, чрез означенията $X = O_{\gamma,\delta}(Y)$, съответно $X \ll_{\gamma,\delta} Y$. 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 $X \asymp Y$.

Ще използваме $\langle x_1, \ldots, x_k \rangle$ за да означаваме наредената k-торка числа $x_1, \ldots, x_k$. С (x, y) ще означаваме най-големия общ делител на x и y, но също и отворен интервал с краища x и y. Съответно $[x, y]$ ще бъде най-малкото общо кратно на x и y, или пък затворен интервал с краища x и y. Точният смисъл ще бъде винаги ясен от контекста. Когато казваме, че някаква функция f е k пъти диференцируема в интервала $[x, y]$ ще считаме, че f е k пъти диференцируема в някакъв отворен интервал, съдържащ $[x, y]$.

Ако $\mathcal{A}$ е крайно множество, то броя на елементите му ще означаваме с $\#\mathcal{A}$ или с $|\mathcal{A}|$.

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

2 Някои леми от математическия анализ

Често се налага да се намира приближена формула за сума от вида

$$\sum_{a<n\le b} f(n), \tag{4}$$

където сумирането е по целите n, а $f(x)$ е комплекснозначна функция, дефинирана за $x \in [a, b]$. Така например, в параграф 4.1 ще се убедим, че изследване на сума от вида (4) се налага при задачи, отнасящи се до преброяването на целите точки в зададена област от равнината.

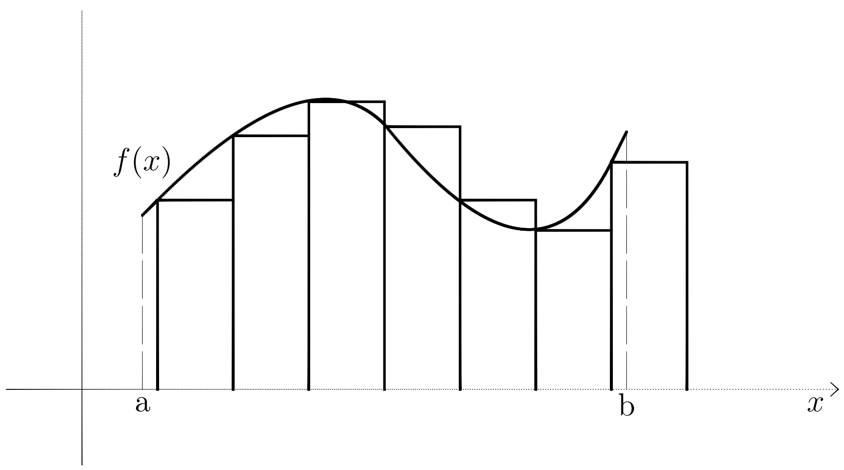
Естествено е да очакваме, че ако функцията $f(x)$ е „достатъчно гладка”, то сумата (4) е приближено равна на интеграла

$$\int_a^b f(x)\,dx. \tag{5}$$

Не е трудно да се оцени грешката, която възниква при замяната на сумата (4) с интеграла (5), при условие, че $f(x)$ е неотрицателна и монотонна. За тази цел се сравнява лицето на криволинейния трапец, определен от условията

$$a < x < b, \qquad 0 < y < f(x)$$

и лицето на многоъгълник. Методът се илюстрира от следния чертеж.



По този начин може да бъде доказана Лема 2.5, формулирана по-долу. Пропускаме разсъжденията, тъй като те могат да се намерят във всеки учебник по диференциално и интегрално смятане.

В настоящата глава ще представим две тъждества, известни като *сумационни формули на Ойлер*. С тяхна помощ грешката, възникваща при замяната на сумата (4) с интеграла (5), се задава в явен вид и може да бъде оценена много по-точно, отколкото чрез метода, който споменахме. Известни са и по-сложни сумационни формули, но в почти всички приложения формулите, които привеждаме в настоящите записки, дават задоволителен резултат.

2.1 Преобразование на Абел

Първо ще изложим една проста, но полезна помощна лема. Тя е известна като *преобразование на Абел* и по-нататък ще бъде често използвана. Както ще видим, с нейна помощ може да бъде доказана първата сумационна формула на Ойлер.

Лема 2.1 (Преобразование на Абел). *Нека $\{\lambda_n\}_{n=1}^{\infty}$ е строго растяща редица от реални числа, за която $\lim_{n\to\infty}\lambda_n = \infty$ и нека $\{g_n\}_{n=1}^{\infty}$ е произволна редица, $g_n \in \mathbb{C}$. Нека $f(x)$ е непрекъснато диференцируема функция в интервала $[a, b]$. Ако*

$$S = \sum_{a<\lambda_n\le b} g_n\, f(\lambda_n),$$

където сумирането се извършва по всички n, за които $a < \lambda_n \le b$, то е в сила тъждеството

$$S = f(b) \sum_{a<\lambda_n\le b} g_n - \int\limits_a^b \left(\sum_{a<\lambda_n\le t} g_n \right) f'(t)\, dt. \tag{6}$$

Забележка. В приложенияга обикновено имаме $\lambda_n = n$.

Доказателство. Да разгледаме интеграла в дясната част на (6). Като сменим реда на сумирането и интегрирането и приложим теоремата на Нютон–Лайбниц, получаваме

$$\begin{aligned}\int\limits_a^b \left(\sum_{a<\lambda_n\le t} g_n \right) f'(t)\, dt &= \sum_{a<\lambda_n\le b} g_n \int\limits_{\lambda_n}^b f'(t)\, dt = \sum_{a<\lambda_n\le b} g_n\, \left(f(b) - f(\lambda_n)\right) \\ &= f(b) \sum_{a<\lambda_n\le b} g_n - S,\end{aligned}$$

с което лемата е доказана.

□

2.2 Първа сумационна формула на Ойлер

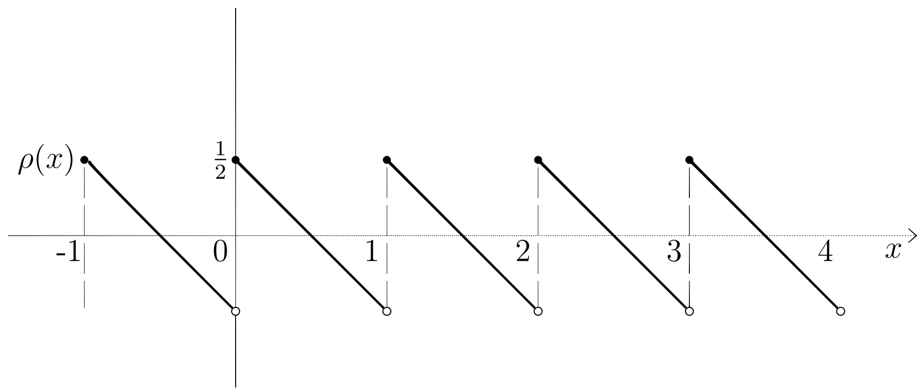
Първо ще дадем следното

Определение 2.2. *При $x \in \mathbb{R}$ означаваме*

$$\rho(x) = \frac{1}{2} - \{x\}, \tag{7}$$

където $\{x\}$ е дробната част на x.

Графиката на $\rho(x)$ е показана на следния чертеж.



Ще изредим някои нейни прости свойства.

Лема 2.3. *Функцията $\rho(x)$ притежава свойствата:*

(1) $\rho(x)$ *е периодична с период 1.*

(2) $|\rho(x)| \le \frac{1}{2}$ *за всяко* $x \in \mathbb{R}$.

(3) $\rho(x)$ *е прекъсната във всяка точка* $m \in \mathbb{Z}$, *като*

$$\lim_{\substack{x\to m\\ x<m}} \rho(x) = -\frac{1}{2}, \qquad \lim_{\substack{x\to m\\ x\ge m}} \rho(x) = \frac{1}{2}.$$

(4) $\rho(x)$ *е диференцируема за всяко* $x \in \mathbb{R}\setminus\mathbb{Z}$, *като* $\rho'(x) = -1$.

Доказателство. Получава се непосредствено от Определение 2.2.

□

Следва първата сумационна формула на Ойлер.

Лема 2.4. *Нека функцията $f(x)$ е непрекъснато диференцируема в интервала $[a, b]$. Тогава е изпълнено*

$$\sum_{a<n\le b} f(n) = \int_a^b f(t)\,dt + \rho(b)f(b) - \rho(a)f(a) - \int_a^b \rho(t)f'(t)\,dt. \tag{8}$$

Доказателство. Прилагаме преобразованието на Абел (Лема 2.1) при $\lambda_n = n$, $g_n = 1$ и използваме очевидното тъждество

$$\sum_{a<n\le t} 1 = [t] - [a] = t - a + \rho(t) - \rho(a),$$

където $\rho(t)$ е функцията от Определение 2.2. Получаваме

$$\begin{aligned}
\sum_{a<n\le b} f(n) &= f(b) \sum_{a<n\le b} 1 - \int_a^b \left(\sum_{a<n\le t} 1\right) f'(t)\,dt \\
&= f(b)\left([b]-[a]\right) - \int_a^b \left([t]-[a]\right) f'(t)\,dt \\
&= f(b)\left(b-a+\rho(b)-\rho(a)\right) - \int_a^b \left(t-a+\rho(t)-\rho(a)\right) f'(t)\,dt \\
&= f(b)\left(b-a+\rho(b)-\rho(a)\right) - \int_a^b \rho(t)\,f'(t)\,dt - \int_a^b \left(t-a-\rho(a)\right) f'(t)\,dt. \qquad (9)
\end{aligned}$$

Чрез интегриране по части намираме, че последният интеграл от горното равенство е равен на

$$\left(t-a-\rho(a)\right) f(t)\Big|_{t=a}^{b} - \int_a^b f(t)\,dt = \left(b-a-\rho(a)\right) f(b) + \rho(a)f(a) - \int_a^b f(t)\,dt.$$

Заместваме този израз в (9) и след прости преобразования, които оставяме на читателя, получаваме (8).

□

Като първо приложение на Лема 2.4 ще получим следната

Лема 2.5. *Нека функцията $f(x)$ е непрекъснато диференцируема, неотрицателна и монотонна в интервала $[a,b]$. Тогава е изпълнено*

$$\left| \sum_{a<n\le b} f(n) - \int_a^b f(x)\,dx \right| \le \max\left(f(a), f(b)\right). \qquad (10)$$

Доказателство. Ако $f(x)$ е монотонно растяща, то $f'(x) \ge 0$ при $a \le x \le b$. Следователно, ако означим с Δ израза в лявата страна на (10), то като използуваме неравенството на триъгълника, Лема 2.3 (2), Лема 2.4 и формулата на Нютон–Лайбниц, получаваме

$$\Delta = \left| \rho(b)f(b) - \rho(a)f(a) - \int_a^b \rho(x)f'(x)\,dx \right| \le \frac{1}{2}\left(f(b) + f(a) + \int_a^b f'(x)\,dx \right) = f(b)$$

Ако $f(x)$ е монотонно намаляваща се разсъждава аналогично.

□

С помощта на Лема 2.5 се получават полезни асимптотични формули. Имаме

Лема 2.6. *Нека $x \geq 2$.*

(1) *Ако $\alpha > -1$, то*

$$\sum_{n \leq x} n^{\alpha} = \frac{x^{\alpha+1}}{\alpha+1} + O_{\alpha}\big(\max(1, x^{\alpha})\big).$$

(2) *Ако $\beta > 1$, то*

$$\sum_{n > x} \frac{1}{n^{\beta}} = \frac{x^{1-\beta}}{\beta-1} + O_{\beta}\big(x^{-\beta}\big).$$

(3) *Имаме*

$$\sum_{n \leq x} \frac{1}{n} = \log x + O(1).$$

(4) *Имаме*

$$\sum_{n \leq x} \log n = x \log x - x + O(\log x).$$

Доказателство. Изчисленията предоставяме на читателя.

□

Като се използуват по-прецизни разсъждения, основани на Лема 2.4, горните резултати могат да бъдат усилени. Например може да се докаже, че

$$\sum_{n \leq x} \frac{1}{n} = \log x + \gamma + O\left(\frac{1}{x}\right), \tag{11}$$

където γ е константата на Ойлер, определена чрез (1). Да отбележим, че съществуването на границата (1) е следствие от формула (11). Може да бъде получена и още по-точна формула за сумата в лявата страна на (11). Такава е приведена в Лема 2.11, която по-долу ще формулираме и докажем.

Като илюстрация, в следващата лема ще усилим резултата от Лема 2.6 (1) за някои от стойностите на параметъра α.

Лема 2.7. *Ако $-1 < \alpha < 0$ и $x \geq 2$, то е в сила формулата*

$$\sum_{n \leq x} n^{\alpha} = \frac{x^{\alpha+1}}{\alpha+1} + c(\alpha) + O(x^{\alpha}), \tag{12}$$

където $c(\alpha)$ зависи само от параметъра α.

Доказателство. Като използуваме Лема 2.4 получаваме

$$\sum_{n \leq x} n^{\alpha} = 1 + \sum_{1 < n \leq x} n^{\alpha} = 1 + \int_1^x t^{\alpha}\, dt + \rho(x) x^{\alpha} - \rho(1) - \alpha \int_1^x \rho(t)\, t^{\alpha-1}\, dt$$

$$= \frac{x^{\alpha+1}}{\alpha+1} + c(\alpha) + \Delta_{\alpha}(x),$$

където

$$c(\alpha) = \frac{1}{2} - \frac{1}{\alpha+1} - \alpha \int\limits_1^\infty \rho(t)\, t^{\alpha-1}\, dt, \qquad \Delta_\alpha(x) = \rho(x)x^\alpha + \alpha \int\limits_x^\infty \rho(t)\, t^{\alpha-1}\, dt.$$

От Лема 2.3 (2) и от условието $-1 < \alpha < 0$ следва

$$|\Delta_\alpha(x)| \le \frac{1}{2}x^\alpha - \frac{\alpha}{2} \int\limits_x^\infty t^{\alpha-1}\, dt = x^\alpha,$$

с което лемата е доказана.

□

2.3 Втора сумационна формула на Ойлер

Въвеждаме още една функция.

Определение 2.8. *За произволно $x \in \mathbb{R}$ полагаме*

$$\sigma(x) = \int\limits_0^x \rho(t)\, dt. \tag{13}$$

Основните ѝ свойства са дадени в следната

Лема 2.9. *Функцията $\sigma(x)$ притежава свойствата:*

(1) *$\sigma(x)$ е периодична с период 1.*

(2) *$0 \le \sigma(x) \le \frac{1}{8}$ за всяко $x \in \mathbb{R}$.*

(3) *$\sigma(x)$ е непрекъсната за всяко $x \in \mathbb{R}$ и диференцируема при $x \in \mathbb{R} \setminus \mathbb{Z}$, като в този случай е изпълнено $\sigma'(x) = \rho(x)$.*

(4) *$\sigma(m) = 0$ при $m \in \mathbb{Z}$.*

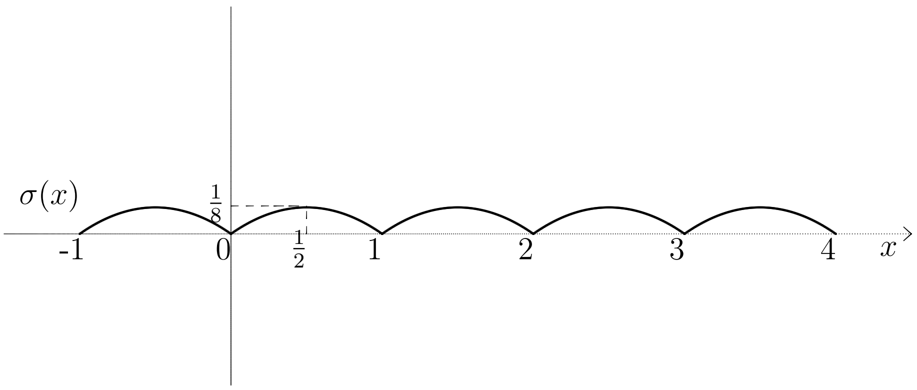
Доказателство. За да докажем (1) използуваме Определения 2.2, 2.8 и също Лема 2.3 (1) и получаваме, че за всяко x е изпълнено

$$\sigma(x+1) - \sigma(x) = \int\limits_x^{x+1} \rho(t)\, dt = \int\limits_0^1 \rho(t)\, dt = \int\limits_0^1 \left(\frac{1}{2} - t\right)\, dt = 0.$$

Останалите свойства следват от свойство (1), Определение 2.8 и от Лема 2.3. Проверката оставяме на читателя.

□

Графиката на $\sigma(x)$ е показана на следния чертеж.



Втората сумационна формула на Ойлер е дадена в следната

Лема 2.10. *Нека функцията $f(x)$ е два пъти непрекъснато диференцируема в интервала $[a, b]$. Тогава е в сила тъждеството*

$$\sum_{a<n\leq b} f(n) = \int_a^b f(t)\,dt + \rho(b)f(b) - \rho(a)f(a) - \sigma(b)f'(b) + \sigma(a)f'(a) + \int_a^b \sigma(t)f''(t)\,dt.$$

Доказателство. При $x \in [a, b]$ определяме функцията

$$F(x) = \int_a^x \big(f(t) + \sigma(t)f''(t)\big)\,dt - \sum_{a<n\leq x} f(n) + \rho(x)f(x) - \sigma(x)f'(x). \tag{14}$$

Първо да разгледаме $F(x)$ при $x \in [a, b] \setminus \mathbb{Z}$. Според теоремата на Нютон–Лайбниц, интегралът в дясната страна на (14) е диференцируема функция на x, чиято производна е равна на $f(x) + \sigma(x)f''(x)$. Очевидно функцията $\sum_{a<n\leq x} f(n)$ е константа в околност на всяка точка от $[a, b]\setminus\mathbb{Z}$, следователно производната ѝ е нула. По-нататък, като използуваме Лема 2.3 (4) виждаме, че $\big(\rho(x)f(x)\big)' = -f(x) + \rho(x)f'(x)$, а от Лема 2.9 (3) следва, че $\big(\sigma(x)f'(x)\big)' = \rho(x)f'(x) + \sigma(x)f''(x)$. Тогава получаваме

$$F'(x) = 0 \qquad \text{при} \qquad x \in [a, b] \setminus \mathbb{Z}.$$

Това означава, че $F(x)$ е константа във всеки непразен интервал от вида

$$[a, b] \cap (m, m+1),$$

където $m \in \mathbb{Z}$. Тази константа, обаче, евентуално зависи от m. Сега ще проверим, че всъщност, за всяко m константата е една и съща. За целта е достатъчно да установим, че $F(x)$ е непрекъсната в целите числа, принадлежащи на $[a, b]$.

Ясно е, че интегралът в дясната страна на (14) е непрекъсната функция на x в интервала $[a, b]$.

Нека $m \in [a, b] \cap \mathbb{Z}$. Тогава очевидно имаме

$$\lim_{\substack{x\to m\\ x<m}} \sum_{a<n\leq x} f(n) = \sum_{a<n\leq m-1} f(n), \qquad \lim_{\substack{x\to m\\ x\geq m}} \sum_{a<n\leq x} f(n) = \sum_{a<n\leq m} f(n),$$

а от Лема 2.3 (3) и от непрекъснатостта на $f(x)$ следва

$$\lim_{\substack{x\to m\\ x<m}} \rho(x)f(x) = -\frac{1}{2}f(m) \qquad \lim_{\substack{x\to m\\ x\geq m}} \rho(x)f(x) = \frac{1}{2}f(m).$$

Накрая, от непрекъснатостта на $f'(x)$ и от Лема 2.9 (3), (4) следва

$$\lim_{x\to m} \sigma(x)f'(x) = \sigma(m)f'(m) = 0.$$

От горните съображения и формули получаваме

$$\lim_{\substack{t\to m\\ t<m}} F(t) = \lim_{\substack{t\to m\\ t\geq m}} F(t) \qquad \text{при} \qquad m \in [a,b] \cap \mathbb{Z}.$$

И така, видяхме, че $F(x)$ е константа в интервала $[a,b]$. Стойността на тази константа е равна на $F(a) = \rho(a)f(a) - \sigma(a)f'(a)$. С това лемата е доказана.

□

Забележка. Лема 2.10 може да бъде доказана и по следния начин. Разбиваме интервала $[a,b]$ на подинтервали посредством последователните цели числа и тогава интегралът $\int_a^b \sigma(t)f''(t)\,dt$ се представя като сума на няколко интеграла. При всеки от тях интегрираме двукратно по части и, като използваме свойствата на функциите $\rho(x)$ и $\sigma(x)$, получаваме желаното тъждество. Описаните методи могат да бъдат използвани и за доказване на Лема 2.4.

Обикновено, като се използува Лема 2.10, се получават по-точни оценки, от тези, които следват от Лема 2.4. С помощта на метода, който използувахме за доказателството на Лема 2.7, ще установим следната

Лема 2.11. *При $x \geq 2$ имаме*

$$\sum_{n\leq x} \frac{1}{n} = \log x + \gamma + \frac{\rho(x)}{x} + O\left(\frac{1}{x^2}\right),$$

където γ е константата на Ойлер.

Доказателство. Като използваме Лема 2.10, получаваме

$$\begin{aligned}
\sum_{n\leq x} \frac{1}{n} &= 1 + \sum_{1<n\leq x} \frac{1}{n} \\
&= 1 + \int_1^x \frac{dt}{t} + \frac{\rho(x)}{x} - \rho(1) - \sigma(x)\left(-\frac{1}{x^2}\right) + \sigma(1)(-1) + \int_1^x \sigma(t)\left(\frac{1}{t}\right)'' dt \\
&= \log x + \frac{\rho(x)}{x} + \frac{1}{2} + \frac{\sigma(x)}{x^2} + 2\int_1^x \frac{\sigma(t)}{t^3}\,dt \\
&= \log x + \gamma_0 + \frac{\rho(x)}{x} + \delta(x), \qquad (15)
\end{aligned}$$

където
$$\gamma_0 = \frac{1}{2} + 2\int\limits_1^\infty \frac{\sigma(t)}{t^3}\,dt, \qquad \delta(x) = \frac{\sigma(x)}{x^2} - 2\int\limits_x^\infty \frac{\sigma(t)}{t^3}\,dt.$$
Тук използувахме, че вследствие на Лема 2.9 (2), интегралът $\int_1^\infty \sigma(t)\,t^{-3}\,dt$ е сходящ.

Ясно е, че от неравенството на триъгълника и от Лема 2.9 (2) следва
$$|\delta(x)| \le \frac{|\sigma(x)|}{x^2} + 2\left|\int\limits_x^\infty \sigma(t)\,t^{-3}\,dt\right| \le \frac{1}{8x^2} + \frac{1}{4}\int\limits_x^\infty \frac{dt}{t^3} = \frac{1}{4x^2}. \tag{16}$$

Остана да отбележим, че от (15), (16) и от опредерението (1) за константата на Ойлер получаваме
$$\gamma_0 = \lim_{x\to\infty}\left(\sum_{n\le x}\frac{1}{n} - \log x\right) = \gamma.$$
С това лемата е доказана.

$\square$

3 Основни понятия и резултати от елементарната теория на числата

3.1 Делимост на числата

Преди да започнем с изложението на основните понятия свързани с понятието делимост, ще отбележим, че множеството на естествените числа $\mathbb{N}$ притежава следните свойствата

(1) *Ако $M \subset \mathbb{N}$ и $M \neq \emptyset$, то M съдържа най-малък елемент.*

(2) *Ако $M \subset \mathbb{N}$ и ако M притежава свойствата*
$1 \in M$,
$n \in M \implies n+1 \in M$,
то $M = \mathbb{N}$.

(3) *Всяка строго намаляваща редица от естествени числа е крайна.*

По-подробна информация може да бъде намерена във всяка книга по основи на математиката. Да отбележим, че горните три свойства са еквиваленти, в смисъл че от кое да е от тях незабавно следват и другите две. Ще споменем също, че (1) е известно като *принцип на добрата наредба* на $\mathbb{N}$, а (2) като *принцип на математическата индукция*. В настоящите записки често ще използваме горните свойства, без да споменаваме изрично това.

Ще формулираме понятието *делимост*.

Определение 3.1. *Нека $a, b \in \mathbb{Z}$ и $a \neq 0$. Казваме, че a дели b и пишем $a \mid b$, ако съществува $c \in \mathbb{Z}$ такова, че $b = ac$. В този случай казваме, че b е кратно на a и, че a е делител на b. Когато a не дели b пишем $a \nmid b$.*

Основните свойства на понятието делимост са изложени в следващата лема, която впоследствие ще използваме многократно, без да цитираме.

Лема 3.2. *Имаме:*

(1) $a \in \mathbb{Z},\ a \neq 0 \implies a \mid a.$

(2) $a, b \in \mathbb{N},\ a \mid b,\ b \mid a \implies a = b.$

(3) $a, b \in \mathbb{Z},\ ab \neq 0,\ a \mid b,\ b \mid a \implies |a| = |b|.$

(4) $a, b, c, \in \mathbb{Z},\ ab \neq 0,\ a \mid b,\ b \mid c \implies a \mid c.$

(5) $a, b \in \mathbb{N},\ a \mid b \implies a \leq b.$

(6) $a, b \in \mathbb{Z},\ ab \neq 0,\ a \mid b \implies |a| \leq |b|.$

(7) $a, b, c \in \mathbb{Z},\ a \neq 0,\ a \mid b \implies a \mid bc.$

(8) $a, b, c \in \mathbb{Z},\ a \neq 0,\ a \mid b,\ a \mid c \implies a \mid (b \pm c).$

Доказателство. Следва директно от Определение 3.1

□

Сега ще определим *най-голям общ делител* и *най-малко общо кратно* на няколко цели числа.

Определение 3.3. *Нека са дадени числата $a_1, \dots, a_n \in \mathbb{Z}$, като поне едно от тях е различно от нула. Казваме, че числото d е общ делител на $a_1, \dots, a_n$, ако $d \mid a_i$ за всяко $i = 1, \dots, n$. Очевидно, измежду всички общи делители на $a_1, \dots, a_n$ има един, който е най-голям. Той се нарича най-голям общ делител на $a_1, \dots, a_n$ и се бележи с $(a_1, \dots, a_n)$.*

Например, най-големия общ делител на числата 4, -10, 18 е $(4, -10, 18) = 2$.

Определение 3.4. *Казваме, че числата $a_1, \dots, a_n$ са взаимно прости, ако*

$$(a_1, \dots, a_n) = 1.$$

Казваме, че числата $a_1, \dots, a_n$ са две по две взаимно прости, ако $(a_i, a_j) = 1$ за всеки i, j, за които $1 \leq i < j \leq n$.

Например, числата 5, 10, 12 са взаимно прости, но не са две по две взаимно прости.

Определение 3.5. *Нека са дадени числата $a_1, \dots, a_n \in \mathbb{Z}$, всяко едно от които е различно от нула. Казваме, че едно число k е общо кратно на $a_1, \dots, a_n$, ако $a_i \mid k$ за всяко $i = 1, \dots, n$. Най-малкото естествено число, което е общо кратно на $a_1, \dots, a_n$ се нарича най-малко общо кратно на $a_1, \dots, a_n$ и се бележи с $[a_1, \dots, a_n]$.*

Например, най-малкото общо кратно на числата -8, 10 и 5 е $[-8, 10, 5] = 40$.

3.2 Прости числа

Определение 3.6. *Нека $n \in \mathbb{N}$ и $n > 1$. Казваме, че числото n е просто, ако не притежава други положителни делители, освен 1 и n. Казваме, че n е съставно, ако то не е просто. Считаме, че числото 1 не е нито просто, нито съставно.*

Например, простите числа по-малки от 50 са 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43 и 47.

От определението на просто число непосредствено следва

Лема 3.7. *Ако $n \in \mathbb{N}$ и $n > 1$, то n притежава прост делител.*

Доказателство. Нека d е най-малкият положителен делител на n, за който $d > 1$. Ако d не е просто, то ще притежава делител $l > 1$. Но тогава $l \mid n$, което противоречи на избора на d. Следователно числото d е просто.

$\square$

Следващото твърдение е в основата на така нареченото *решето на Ератостен*. Чрез него, ако са ни известни простите числа, ненадминаващи $\sqrt{x}$, намираме лесно простите числа от интервала $(\sqrt{x}, x]$.

Лема 3.8. *Ако числото $n \in \mathbb{N}$ е съставно, то притежава прост делител p такъв, че $p \leq \sqrt{n}$.*

Доказателство. Тъй като n е съставно, то $n = km$, където $k, m \in \mathbb{N}$, $k, m > 1$. Нека е изпълнено, например, $k \leq m$. Според Лема 3.7 числото k притежава прост делител p и очевидно имаме $p \leq k \leq m$. Тогава $p^2 \leq km = n$, с което лемата е доказана.

$\square$

Още от древността е известна следната основна

Теорема 3.9 (Евклид)**.** *Съществуват безбройно много прости числа.*

Доказателство. Допускаме, че има само краен брой прости числа и нека те са $p_1, p_2, \ldots, p_k$. Разглеждаме числото $Q = p_1 p_2 \ldots p_k + 1$. От Лема 3.7 следва, че Q притежава прост делител p. Но тогава, вследствие на нашето допускане, числото p съвпада с някое от числата $p_1, \ldots, p_k$, откъдето виждаме, че p дели $p_1 \ldots p_k = Q - 1$. Но тогава p е делител на две последователни естествени числа, което е невъзможно.

$\square$

Следващото важно свойство е известно като *Основна теорема на аритметиката.*

Теорема 3.10. *Всяко естествено число по-голямо от 1 се разлага на произведение от прости множители, и то еднозначно с точност до реда на тези множители.*

Доказателство. Първо ще докажем съществуване на разлагането. Допускаме противното, а именно че някои естествени числа по-големи от 1 не могат да се разложат на прости множители. Нека n е най-малкото такова число. Ясно е, че n е съставно, следователно $n = km$, където $k, m \in \mathbb{N}$, $1 < k, m < n$. Но според избора на n, всяко от числата k и m се разлага на прости множители, откъдето следва, че n също притежава такова разлагане. Получихме противоречие, с което съществуването на разлагане е доказано.

Сега да допуснем, че някои естествени числа по-големи от 1 се разлагат поне по два различни начини на произведение на прости множители. Нека n е най-малкото такова число и нека

$$n = p_1 \ldots p_k = q_1 \ldots q_t, \tag{17}$$

където p_i, q_j са прости числа, като двете представяния не могат да се получат едно от друго чрез пренареждане на множителите.

Първо отбелязваме, че $k > 1$ и $t > 1$. Наистина, да допуснем например, че $k = 1$. Тогава n е просто число и ще имаме $t = 1$. Следователно двете представяния на n съвпадат, което противоречи на избора на това число.

Сега ще видим, че кое да е от числата p_i е различно от всяко от числата q_j. Наистина, да допуснем например, че $p_1 = q_1$. Тогава числото $n' = n/p_1$ удовлетворява $1 < n' < n$ и в същото време притежава две различни разлагания на прости множители, което противоречи на избора на n.

Тъй като $p_1 \neq q_1$, то без ограничение на общостта можем да считаме, че $p_1 < q_1$. Разглеждаме числото

$$l = n - p_1 q_2 \dots q_t = q_1 q_2 \dots q_t - p_1 q_2 \dots q_t = (q_1 - p_1)\, q_2 \dots q_t. \tag{18}$$

От определението на l и от (17) виждаме, че

$$l = p_1 p_2 \dots p_k - p_1 q_2 \dots q_t = p_1 (p_2 \dots p_k - q_2 \dots q_t),$$

следователно $p_1 \mid l$. Тъй като $1 < l < n$, то като си припомним избора на n, правим заключението, че числото l се разлага еднозначно на прости множители и p_1 е някой от тях. Ако $q_1 - p_1 = 1$, то от равенството (18) следва, че p_1 съвпада с някое от числата $q_2, \dots, q_t$, което не е възможно. Ако пък $q_1 - p_1 > 1$, то $q_1 - p_1$ се разлага еднозначно на прости множители и p_1 е един от тях. Следователно $p_1 \mid (q_1 - p_1)$, откъдето $p_1 \mid q_1$ и $p_1 = q_1$. Получаваме противоречие, с което единствеността на разлагането на прости множители е доказана.

$\square$

От тази теорема веднага получаваме

Следствие 3.11. *Всяко $n \in \mathbb{N}$ се представя еднозначно във вида*

$$n = \prod_p p^{l(n,p)},$$

където произведението е по всички прости числа p и $l(n,p)$ са неотрицателни цели числа, които са различни от нула само за краен брой p.

$\square$

Определение 3.12. *Нека $n \in \mathbb{N}$. Представянето на n от Следствие 3.11 се нарича негово канонично разлагане на прости множители.*

Наример, каноничното разлагане на числото 60 е $60 = 2^2 \cdot 3 \cdot 5$.

От Теорема 3.10 непосредствено следва

Лема 3.13. *Ако числото $n \in \mathbb{N}$ притежава канонично разлагане $n = p_1^{k_1} \dots p_m^{k_m}$, то положителните делители на n са точно числата $p_1^{\nu_1} \dots p_m^{\nu_m}$, където $0 \leq \nu_j \leq k_j$, $1 \leq j \leq m$.*

□

В сила е също следната важна

Лема 3.14. *Нека $n, k, m \in \mathbb{N}$. Ако $n \mid km$ и $(n, k) = 1$, то $n \mid m$.*

Доказателство. Нека p е произволен прост делител на n и нека p влиза в каноничното му разлагане в степен ν. Тъй като $n \mid km$, то p влиза в каноничното разлагане на km в степен μ такава, че $\mu \geq \nu$. Но $(n, k) = 1$, откъдето $p \nmid k$, следователно p влиза в каноничното разлагане на m в степен μ. Оттук следва, че $n \mid m$.

□

Ако са известни каноничните разлагания на няколко естествени числа, то техният най-голям общ делител и тяхното най-малко общо кратно се намират лесно. В сила е следната

Лема 3.15. *Нека $a_1, \dots a_n \in \mathbb{N}$. Ако*

$$a_i = \prod_p p^{l(a_i,p)}, \qquad 1 \leq i \leq n,$$

са каноничните разлагания на тези числа, то

$$(a_1, \dots, a_n) = \prod_p p^{\delta(p)}, \qquad [a_1, \dots, a_n] = \prod_p p^{\kappa(p)},$$

където

$$\delta(p) = \min \left(l(a_1, p), \dots, l(a_n, p) \right), \qquad \kappa(p) = \max \left(l(a_1, p), \dots, l(a_n, p) \right).$$

Доказателство. Следва от Определения 3.3, 3.5 и от Теорема 3.10.

□

Например, като използваме, че $60 = 2^2 \cdot 3 \cdot 5$ и $100 = 2^2 \cdot 5^2$, намираме

$$(60, 100) = 2^2 \cdot 5 = 20, \qquad [60, 100] = 2^2 \cdot 3 \cdot 5^2 = 300.$$

3.3 Аритметични функции

Определение 3.16. *Всяка функция $f : \mathbb{N} \to \mathbb{C}$ се нарича аритметична функция.*

Произволна функция, определена в множество съдържащо $\mathbb{N}$ може да се разглежда и като аритметична функция. Такива са например функциите $\mathbf{1}$, $\mathbf{I}$ и $\mathbf{log}$, определени за всяко $n \in \mathbb{N}$ чрез равенствата

$$\mathbf{1}(n) = 1, \qquad \mathbf{I}(n) = n, \qquad \mathbf{log}(n) = \log n. \tag{19}$$

Удобно е също така да определим

$$\mathbf{c}(n) = \begin{cases} 1 & \text{ако} \quad n = 1, \\ 0 & \text{ако} \quad n > 1. \end{cases} \tag{20}$$

Ще дефинираме някои други често срещани функции.

Определение 3.17. *Означаваме с $\tau(n)$ броят на положителните делители на числото n, т.е.*

$$\tau(n) = \sum_{d|n} 1. \tag{21}$$

Определение 3.18. *Означаваме със $\sigma(n)$ сумата от положителните делители на числото n, т.е.*

$$\sigma(n) = \sum_{d|n} d. \tag{22}$$

Забележка. Буквата σ използувахме още за означаване на функцията от Определение 2.8. Това няма да предизвика объркване, тъй като при всяка употреба смисълът е ясен от контекста.

Определение 3.19. *Определяме функцията на Мьобиус чрез равенството*

$$\mu(n) = \begin{cases} 1 & \text{ако } n = 1, \\ (-1)^k & \text{ако } n \text{ е произведение на } k \text{ различни прости числа,} \\ 0 & \text{за останалите } n. \end{cases} \tag{23}$$

Определение 3.20. *Функцията на Ойлер $\varphi(n)$ се определя като броя на естествените числа $k \le n$, които са взаимно прости с n, т.е.*

$$\varphi(n) = \sum_{\substack{k=1 \\ (k,n)=1}}^{n} 1 \tag{24}$$

Определение 3.21. *За всяко $n \in \mathbb{Z}$, $n \ge 0$ определяме $r(n)$ като броя наредените двойки $\langle x, y \rangle \in \mathbb{Z}^2$, за които е изпълнено $x^2 + y^2 = n$.*

Например имаме $r(0) = 1$, $r(1) = 4$, $r(2) = 4$, $r(3) = 0$, $r(4) = 4$.

Определение 3.22. *Функцията на Манголд $\Lambda(n)$ определяме чрез формулата*

$$\Lambda(n) = \begin{cases} \log p & \text{при } n = p^k, \text{ където } p \text{ е просто и } k \in \mathbb{N}; \\ 0 & \text{за останалите } n. \end{cases} \tag{25}$$

Например имаме

$$\Lambda(1) = 0, \quad \Lambda(2) = \log 2, \quad \Lambda(3) = \log 3, \quad \Lambda(4) = \log 2, \quad \Lambda(5) = \log 5, \quad \Lambda(6) = 0.$$

Сега ще въведем една важна операция, която на всеки две аритметични функции съпоставя трета.

Определение 3.23. *На всяка двойка аритметични функции f и g съпоставяме функцията $h = f * g$, която се нарича конволюция на Дирихле и се определя чрез формулата*

$$h(n) = \sum_{dm=n} f(d)g(m). \tag{26}$$

(Сумирането е по всички наредени двойки $\langle d, m\rangle \in \mathbb{N}^2$, удовлетворяващи условието $dm = n$).

Ясно е, че формула (26) може да се запише още във вида

$$h(n) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right) \tag{27}$$

В частност, ако **1** е функцията, определена чрез (19), то

$$(f * \mathbf{1})(n) = \sum_{d|n} f(d),$$

се нарича *функция сума* на f.

Чрез операцията $*$ редица формули могат да се запишат в по-компактен вид. Така например функциите $\tau(n)$ и $\sigma(n)$ удовлетворяват

$$\tau = \mathbf{1} * \mathbf{1}, \qquad\qquad \sigma = \mathbf{I} * \mathbf{1}, \tag{28}$$

където **1** и **I** са зададени чрез (19). Освен това, ако се използува това означение, доказателствата на редица тъждества се опростяват значително.

Ще установим някои от свойствата на конволюцията на Дирихле.

Лема 3.24. *Операцията $*$, определена в множеството на аритметичните функции, е комутативна и асоциативна, т.е.*

$$f * g = g * f, \qquad (f * g) * h = f * (g * h). \tag{29}$$

Ако **c** *е функцията, определена чрез* (20)*, то за всяка аритметична функция f е изпълнено*

$$f * \mathbf{c} = f. \tag{30}$$

Доказателство Комутативността на операцията $*$ е очевидна. За да докажем нейната асоциативност, използуваме равенствата

$$\begin{aligned}((f * g) * h)(n) &= \sum_{dm=n} (f * g)(d)\, h(m) = \sum_{dm=n} \left(\sum_{kl=d} f(k)g(l)\right) h(m) \\ &= \sum_{klm=n} f(k)g(l)h(m) = \sum_{kr=n} f(k)\left(\sum_{lm=r} g(l)h(m)\right) \\ &= \sum_{kr=n} f(k)\,(g * h)(r) = (f * (g * h)(n).\end{aligned}$$

С това формулите (29) са установени. Формула (30) следва непосредствено от (20) и от (26).

□

Ще определим клас от аритметични функции — този на мултипликативните функции.

Определение 3.25. *Казваме, че аритметичната функция $f(n)$ е мултипликативна, ако $f(1) = 1$ и ако $f(n_1 n_2) = f(n_1) f(n_2)$ при $n_1, n_2 \in \mathbb{N}, (n_1, n_2) = 1$.*

Такива са например функциите $\mathbf{1}$, $\mathbf{I}$, $\mathbf{c}$, определени чрез (19) и (20). Имаме също

Лема 3.26. *Функцията на Мьобиус $\mu(n)$ е мултипликативна.*

Доказателство. Следва непосредствено от Определения 3.19 и 3.25.

□

Като се използува Определение 3.25, лесно се получава следната лема, която, макар и проста, е твърде полезна за доказване на тъждества, в които участват мултипликативни функции.

Лема 3.27. *Две мултипликативни функции съвпадат, ако приемат еднакви стойности когато аргументът е степен на просто число.*

Доказателство. Използуваме, че ако функцията f е мултипликативна и $n = p_1^{k_1} \dots p_m^{k_m}$ е каноничното разлагане на числото n, то $f(n) = f\left(p_1^{k_1}\right) \dots f\left(p_m^{k_m}\right)$.

□

Подклас на класа на мултипликативните функции е този на напълно мултипликативните функции.

Определение 3.28. *Казваме, че аритметичната функция $f(n)$ е напълно мултипликативна, ако $f(1) = 1$ и ако $f(n_1 n_2) = f(n_1) f(n_2)$ при всички $n_1, n_2 \in \mathbb{N}$.*

От (19), (20) и Определение 3.28 веднага получаваме

Лема 3.29. *Функциите* $\mathbf{1}$, $\mathbf{I}$ *и* $\mathbf{c}$, *определени чрез* (19) *и* (20), *са напълно мултипликативни.*

□

Пример на мултипликативна функция, която не е напълно мултипликативна е функцията на Мьобиус $\mu(n)$.

Следващата лема ни дава възможност да констуираме нови мултипликативнни функции от зададени такива.

Лема 3.30. *Нека аритметичните функции f и g са мултипликативни. Тогава и функцията $h = f * g$ е мултипликативна.*

Доказателство. Очевидно

$$h(1) = \sum_{dm=1} f(d)g(m) = f(1)g(1) = 1.$$

Нека $n_1, n_2 \in \mathbb{N}$, като $(n_1, n_2) = 1$. От Лема 3.13 следва, че положителните делители на $n_1 n_2$ са точно числата $d_1 d_2$, където d_1 пробягва положителните делители на n_1, а d_2 — на n_2. Тогава, като използуваме, че f и g са мултипликативни, получаваме

$$\begin{aligned}
h(n_1 n_2) &= \sum_{d \mid n_1 n_2} f(d)\, g\left(\frac{n_1 n_2}{d}\right) = \sum_{d_1 \mid n_1} \sum_{d_2 \mid n_2} f(d_1 d_2)\, g\left(\frac{n_1 n_2}{d_1 d_2}\right) \\
&= \sum_{d_1 \mid n_1} \sum_{d_2 \mid n_2} f(d_1) f(d_2)\, g\left(\frac{n_1}{d_1}\right) g\left(\frac{n_2}{d_2}\right) \\
&= \left(\sum_{d_1 \mid n_1} f(d_1)\, g\left(\frac{n_1}{d_1}\right) \right) \left(\sum_{d_2 \mid n_2} f(d_2)\, g\left(\frac{n_2}{d_2}\right) \right) \\
&= h(n_1) h(n_2).
\end{aligned}$$

□

Следствие 3.31. *Ако функцията f е мултипликативна, то нейната функция сума $f * \mathbf{1}$ също е мултипликативна.*

□

Да отбележим, че ако f и g са напълно мултипликативни, то $f*g$ не е непременно такава. Например $\tau = \mathbf{1} * \mathbf{1}$ не е напълно мултипликативна.

Следващата лема ни дава възможност да изчисляваме $\tau(n)$ и $\sigma(n)$, ако ни е известно каноничното разлагане на числото n.

Лема 3.32. *Функциите $\tau(n)$ и $\sigma(n)$ са мултипликативни. Ако $n = p_1^{k_1} \dots p_m^{k_m}$ е каноничното разлагане на числото n, то*

$$\tau(n) = (k_1 + 1) \dots (k_m + 1), \qquad \sigma(n) = \prod_{i=1}^{m} \frac{p_i^{k_i+1} - 1}{p_i - 1}.$$

Доказателство. Следва от (28), Лема 3.29 и Лема 3.30

□

Ще приложим последната лема, за да оценим отгоре функцията $\tau(n)$.

Лема 3.33. *При $n \in \mathbb{N}$ и при произволно $\varepsilon > 0$ е изпълнено*

$$\tau(n) \ll_\varepsilon n^\varepsilon. \tag{31}$$

Доказателство. Можем да считаме, че $n > 1$ и нека $n = p_1^{k_1} \dots p_m^{k_m}$ е каноничното му разлагане на прости множители. Тогава от Лема 3.32 следва

$$\frac{\tau(n)}{n^\varepsilon} = \prod_{i=1}^{m} \frac{k_i + 1}{p_i^{\varepsilon k_i}} = P_1 \, P_2, \tag{32}$$

където P_1 е произведението по тези i, за които $p_i^\varepsilon \le 2$, а P_2 е произведението на останалите множители.

Да разгледаме произволен множител от произведението P_1. Знаем, че

$$2^x = e^{x \log 2} > x \log 2 \qquad \text{при} \qquad x > 0.$$

Тогава всеки такъв множител удовлетворява

$$\frac{k_i + 1}{p_i^{\varepsilon k_i}} \le \frac{2k_i}{p_i^{\varepsilon k_i}} \le \frac{2k_i}{2^{\varepsilon k_i}} \le \frac{2k_i}{\varepsilon k_i \log 2} = \frac{2}{\varepsilon \log 2}.$$

От друга страна, броят на простите числа p, за които $p^\varepsilon \le 2$ не надхвърля $2^{1/\varepsilon}$. Тогава

$$P_1 \le \left(\frac{2}{\varepsilon \log 2} \right)^{2^{1/\varepsilon}}. \tag{33}$$

Да разгледаме множител от произведението P_2. За такъв имаме $p_i^\varepsilon > 2$ и, тъй като $2^k \ge k + 1$ при $k \in \mathbb{N}$, то

$$\frac{k_i + 1}{p_i^{\varepsilon k_i}} \le \frac{k_i + 1}{2^{k_i}} \le 1.$$

Оттук следва, че

$$P_2 \le 1. \tag{34}$$

Като използуваме (32) – (34) получаваме

$$\tau(n) \le C(\varepsilon) \, n^\varepsilon, \qquad C(\varepsilon) = \left(\frac{2}{\varepsilon \log 2} \right)^{2^{1/\varepsilon}},$$

с което оценката за $\tau(n)$ от (31) е доказана.

$\square$

За приложенията оценката от горната лема е достатъчно точна, но ще отбележим, че тя може да бъде усилена. Може да се докаже, че ако $\varepsilon > 0$ е произволно, то при достатъчно големи n е изпълнено

$$\tau(n) \le 2^{(1+\varepsilon) \frac{\log n}{\log \log n}}.$$

Последната оценка е, в известен смисъл, неподобряема. По-точно, ако заменим израза $1+\varepsilon$ в показателя с $1-\varepsilon$, то полученото неравенство не е вярно за безбройно много стойности на n.

Следва едно от основните свойства на функцията на Мьобиус. То се прилага при решаването на много задачи, тъй като дава възможност „да се отдели” числото 1 от останалите естествени числа.

Лема 3.34. *Ако μ е функцията на Мъобиус, определена чрез* (23)*, а* $\mathbf{1}$ *и* $\mathbf{c}$ *са функциите, определени чрез* (19) *и* (20)*, то*

$$\mu * \mathbf{1} = \mathbf{c}. \tag{35}$$

Доказателство. Първо да отбележим, че равенството (35) може да се запише във вида

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{при } n = 1, \\ 0 & \text{при } n > 1. \end{cases} \tag{36}$$

При $n = 1$ равенството (36) е изпълнено. Ако $n = p^k$, където p е просто число и $k \in \mathbb{N}$, то равенството също е вярно, тъй като $\mathbf{c}(p^k) = 0$ и

$$(\mu * \mathbf{1})(p^k) = \sum_{d|p^k} \mu(d) = \sum_{l=0}^{k} \mu(p^l) = \mu(1) + \mu(p) = 1 - 1 = 0.$$

Остава да приложим Лема 3.27 и, тъй като функциите от двете страни на (36) са мултипликативни, то лемата е доказана.

□

Следва известната *формула на Мъобиус за обръщане.*

Лема 3.35. *Нека μ е функцията на Мъобиус и нека* $\mathbf{1}$ *е функцията, определена чрез* (19)*. Ако f и g са произволни аритметични функции, то равенствата*

$$f = g * \mathbf{1} \tag{37}$$

и

$$g = f * \mu \tag{38}$$

са еквивалентни.

Доказателство. Ако е изпълнено (37), то като използваме Лема 3.24 и Лема 3.34, получаваме

$$f * \mu = (g * \mathbf{1}) * \mu = g * (\mathbf{1} * \mu) = g * \mathbf{c} = g.$$

Ако пък е налице (38), то имаме

$$g * \mathbf{1} = (f * \mu) * \mathbf{1} = f * (\mu * \mathbf{1}) = f * \mathbf{c} = f.$$

□

Изложеното доказателство илюстрира ползата от въвеждането на операцията „конволюция на Дирихле” и изучаването на нейните свойства. Да отбележим също, че Лема 3.34 се формулира обикновено по следния начин:

Ако f и g са аритметични функции, то равенствата

$$f(n) = \sum_{d|n} g(d), \qquad g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right)$$

са еквивалентни.

Според формула (30) от Лема 3.24, функцията $\mathbf{c}$, определена чрез (20), играе ролята на единица относно операцията $*$. Следващата лема ни дава отговор на въпроса кои функции са обратими относно тази операция.

Лема 3.36. *Ако f е аритметична функция такава, че $f(1) \neq 0$, то съществува единствена аритметична функция g, удовлетворяваща равенството*

$$f * g = \mathbf{c}. \tag{39}$$

Освен това, ако f е мултипликативна, то g също е мултипликативна.

Доказателство. Ще дефинираме функцията g индуктивно по такъв начин, че за всяко $n \in \mathbb{N}$ да е изпълнено

$$\sum_{dm=n} f(d)g(m) = \begin{cases} 1 & \text{при } n = 1, \\ 0 & \text{при } n > 1. \end{cases} \tag{40}$$

Определяме $g(1) = f(1)^{-1}$ и тогава (40) е вярно при $n = 1$.

Ако $n > 1$ и ако сме определили $g(m)$ при $m < n$, то определяме $g(n)$ чрез

$$g(n) = -f(1)^{-1} \sum_{\substack{dm=n \\ m<n}} f(d)g(m).$$

Ясно е, че така конструираната функция g удовлетворява (40).

Сега ще се убедим, че съществува единствена функция g притежаваща указаното свойство. Наистина, ако допуснем, че g_1 е друга такава и разгледаме функцията $G(n) = g(n) - g_1(n)$, то за всяко $n \in \mathbb{N}$ ще имаме

$$\sum_{dm=n} f(d)G(m) = 0. \tag{41}$$

Тогава $f(1)G(1) = 0$, откъдето $G(1) = 0$. Ако $n > 1$ и ако сме доказали, че $G(m) = 0$ при $m < n$, то от (41) получаваме също, че $G(n) = 0$. Следователно, като използваме принципа на математическата индукция, виждаме, че G е тъждествено равна на нула, което означава, че функцията g_1 съвпада с g.

Нека сега функцията f е мултипликативна и нека g е определена чрез (40). От условието $f(1) = 1$ следва
$$g(1) = 1. \tag{42}$$
Имаме също
$$\sum_{d|n} f(d)\, g\left(\frac{n}{d}\right) = 0 \qquad \text{при} \qquad n > 1. \tag{43}$$

Да допуснем, че g не е мултипликативна. Тогава съществуват $n_1, n_2 \in \mathbb{N}$ удовлетворяващи $(n_1, n_2) = 1$, но такива че $g(n_1 n_2) \neq g(n_1)g(n_2)$. От всички тези наредени двойки n_1, n_2 избираме такава, че произведението $n_1 n_2$ да е минимално и оттук нататък считаме, че n_1, n_2 удовлетворяват и това условие. Оттук следва $n_1 > 1$ и $n_2 > 1$.

От (42), (43) и от избора на n_1, n_2 имаме
$$\begin{aligned}
0 &= \sum_{d|n_1 n_2} f(d)\, g\left(\frac{n_1 n_2}{d}\right) \\
&= g(n_1 n_2) + \sum_{\substack{d_1|n_1 \\ d_2|n_2 \\ d_1 d_2 > 1}} f(d_1 d_2)\, g\left(\frac{n_1 n_2}{d_1 d_2}\right) \\
&= g(n_1 n_2) + \sum_{\substack{d_1|n_1 \\ d_2|n_2 \\ d_1 d_2 > 1}} f(d_1)\, f(d_2)\, g\left(\frac{n_1}{d_1}\right)\, g\left(\frac{n_2}{d_2}\right) \\
&= g(n_1 n_2) - g(n_1)g(n_2) + \left(\sum_{d_1|n_1} f(d_1)\, g\left(\frac{n_1}{d_1}\right)\right) \left(\sum_{d_2|n_2} f(d_2)\, g\left(\frac{n_2}{d_2}\right)\right) \\
&= g(n_1 n_2) - g(n_1)g(n_2).
\end{aligned}$$
От последната формула следва $g(n_1 n_2) = g(n_1)g(n_2)$, което противоречи на избора на n_1, n_2. Тогава нашето допускане е погрешно, т.е. g е мултипликативна. С това лемата е доказана.

□

Следващата лема предствлява обобщение на Лема 3.36 и допълва Лема 3.30.

Лема 3.37. *Ако са дадени аритметичните функции f и h и ако $f(1) \neq 0$, то съществува единствена аритметична функция g такава, че $f * g = h$. Освен това, ако f и h са мултипликативни, то и g е мултипликативна.*

Доказателство. Като използваме Лема 3.36 намираме функция ρ такава, че $f * \rho = \mathbf{c}$, където $\mathbf{c}$ е определена от (20). Тогава, ако $g = \rho * h$, то като използваме Лема 3.24 виждаме, че

$$f * g = f * (\rho * h) = (f * \rho) * h = \mathbf{c} * h = h.$$

По-нататък, ако $f * g = h$, то

$$\rho * h = \rho * (f * g) = (f * \rho) * g = \mathbf{c} * g = g,$$

с което единствеността на g е доказана. Накрая, ако f е мултипликативна, то според Лема 3.36 и функцията ρ, определена по-горе, е мултипликативна. Тогава, като използваме Лема 3.30, виждаме, че и $g = \rho * h$ е мултипликативна.

$\square$

Горните леми ни дават възможност да получим още някои важни свойства на аритметичните функции, въведени досега. Да разгледаме функцията на Ойлер, определена чрез (24). Имаме

Лема 3.38. *За всяко $n \in \mathbb{N}$ е изпълнено*

$$\varphi(n) = n \sum_{d|n} \frac{\mu(d)}{d}. \tag{44}$$

Доказателство. Като използваме (24) и (36), получаваме

$$\varphi(n) = \sum_{\substack{1 \le k \le n \\ (k,n)=1}} 1 = \sum_{1 \le k \le n} \sum_{d|(k,n)} \mu(d).$$

Сега, като сменим реда на сумиране, намираме

$$\varphi(n) = \sum_{d|n} \mu(d) \sum_{\substack{1 \le k \le n \\ d|k}} 1 = \sum_{d|n} \mu(d) \, \frac{n}{d} = n \sum_{d|n} \frac{\mu(d)}{d}.$$

$\square$

Лема 3.39. *Функцията на Ойлер е мултипликативна.*

Доказателство. Тъй като функцията $\mu(n)$ е мултипликативна, то и функцията $\frac{\mu(n)}{n}$ е такава. Но тогава, според Следствие 3.31, мултипликативна е и функцията $\sum_{d|n} \frac{\mu(d)}{d}$. Следователно, като използваме (44), получаваме, че $\varphi(n)$ също е мултипликативна.

$\square$

Лема 3.40. *При всяко $n \in \mathbb{N}$ е в сила тъждеството*

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right),$$

където произведението е по всички прости делители на n.

Доказателство. Да разгледаме функциите

$$\prod_{p|n}\left(1-\frac{1}{p}\right) \qquad \text{и} \qquad \sum_{d|n}\frac{\mu(d)}{d}=\frac{\varphi(n)}{n}.$$

Те са мултипликативни и приемат равни стойности, когато n е степен на просто число. Следователно, според Лема 3.27, тези функции са тъждествено равни.

□

Лема 3.41. *За всяко $n \in \mathbb{N}$ е изпълнено*

$$\frac{n}{\varphi(n)}=\sum_{d|n}\frac{\mu^2(d)}{\varphi(d)}. \tag{45}$$

Доказателство. Функциите от двете страни на (45) са мултипликативни, следователно достатъчно е да проверим това равенство когато n е степен на просто число. Изчисленията оставяме на читателя.

□

Сега да разгледаме функцията на Манголд, определена чрез (25). Нейни важни свойства са дадени в следващите две леми.

Лема 3.42. *Функциите* $\mathbf{1}$*,* $\mathbf{log}$ *и* Λ*, определени чрез* (19) *и* (25) *са свързани с равенството*

$$\Lambda*\mathbf{1}=\mathbf{log}. \tag{46}$$

Доказателство. Трябва да проверим, че за всяко $n \in \mathbb{N}$ е изпълнено

$$\sum_{d|n}\Lambda(d)=\log n. \tag{47}$$

При $n=1$ равенството (47) е очевидно. Нека $n>1$ и нека n притежава канонично разлагане $n=p_1^{k_1}\dots p_m^{k_m}$. От определението на функцията на Манголд следва, че ако $d \mid n$ и $\Lambda(d)\neq 0$, то $d=p_j^{\nu_j}$, където $1\le j\le m$, $1\le \nu_j\le k_j$. Тогава имаме

$$\begin{aligned}\sum_{d|n}\Lambda(d)&=\sum_{\nu_1=0}^{k_1}\cdots\sum_{\nu_m=0}^{k_m}\Lambda(p_1^{\nu_1}\dots p_m^{\nu_m})=\sum_{j=1}^{m}\sum_{\nu=1}^{k_j}\Lambda(p_j^{\nu})\\&=\sum_{j=1}^{m}\sum_{\nu=1}^{k_j}\log p_j=\sum_{j=1}^{m}k_j\log p_j=\log(p_1^{k_1}\dots p_m^{k_m})=\log n.\end{aligned}$$

□

Лема 3.43. *При всяко $n \in \mathbb{N}$ е изпълнено*

$$\Lambda(n)=\sum_{d|n}\mu(d)\log\frac{n}{d}, \tag{48}$$

$$\Lambda(n)=-\sum_{d|n}\mu(d)\log d. \tag{49}$$

Доказателство. Равенството (48) е следствие от Лема 3.35 и Лема 3.42, а (49) се получава от (48) и Лема 3.34.

□

Следва едно полезно тъждество за функцията на Мьобиус, което ни дава възможност да решаваме задачи, свързани с безквадратни числа (т.е. числа, всички прости делители на които влизат в каноничното им разлагане в първа степен).

Лема 3.44. *При всяко $n \in \mathbb{N}$ е изпълнено*

$$\mu^2(n) = \sum_{d^2 | n} \mu(d). \tag{50}$$

Сумирането е по естествените числа d, за които $d^2 \mid n$.

Доказателство. Може да се проведе, като се установи, че функциите от двете страни на (50) са мултипликативни и приемат еднакви стойности, при стойност на аргумента равна на степен на просто число. Изчисленията оставяме на читателя.

□

Накрая ще изложим важен резултат, известен като *тъждество на Ойлер.* Той е в основата на мултипликативна теория на числата.

Теорема 3.45 (Ойлер)**.** *Ако функцията $\lambda(n)$ е мултипликативна и ако редът*

$$\sum_{n=1}^{\infty} \lambda(n) \tag{51}$$

е абсолютно сходящ, то е в сила тъждеството

$$\sum_{n=1}^{\infty} \lambda(n) = \prod_{p} T_p, \tag{52}$$

където произведението е по всички прости числа и

$$T_p = 1 + \lambda(p) + \lambda(p^2) + \dots . \tag{53}$$

Ако, освен това, функцията $\lambda(n)$ е напълно мултипликативна, то

$$\sum_{n=1}^{\infty} \lambda(n) = \prod_{p} \left(1 - \lambda(p)\right)^{-1} \tag{54}$$

Доказателство. Първо да отбележим, че от абсолютната сходимост на реда (51) следва, че редът (53) също е абсолютно сходящ. При произволно реално $x \geq 2$ разглеждаме произведението

$$P(x) = \prod_{p \leq x} T_p.$$

Тогава, ако простите числа ненадминаващи x са $p_1, p_2, \ldots, p_l$, то като използуваме познатата теорема за умножаване на краен брой абсолютно сходящи редове и също условието за мултипликативност на функцията $\lambda(n)$, получаваме

$$P(x) = \prod_{i=1}^{l} T_{p_i} = \sum_{k_1=0}^{\infty} \cdots \sum_{k_l=0}^{\infty} \lambda\big(p_1^{k_1}\big) \ldots \lambda\big(p_l^{k_l}\big) = \sum_{k_1=0}^{\infty} \cdots \sum_{k_l=0}^{\infty} \lambda\big(p_1^{k_1} \ldots p_l^{k_l}\big).$$

От горното равенство и от основната теорема на аритметиката (Теорема 3.10) виждаме, че

$$P(x) = {\sum}' \lambda(n),$$

където сумирането е по всички $n \in \mathbb{N}$, простите делители на които са измежду числата $p_1, \ldots, p_l$, т.е. не надминават x. Но ако $n \leq x$, то всички негови прости делители не надхвърлят x. Тогава получаваме

$$P(x) = \sum_{n \leq x} \lambda(n) + \Delta(x), \tag{55}$$

където

$$\Delta(x) = \sum_{\substack{n > x \\ p \mid n \,\Rightarrow\, p \leq x}} \lambda(n).$$

Оттук следва

$$|\Delta(x)| \leq \sum_{n > x} |\lambda(n)|$$

и, като вземем предвид, че редът (51) е абсолютно сходящ, намираме

$$\lim_{x \to \infty} \Delta(x) = 0.$$

Тогава, ако в равенство (55) извършим граничен преход $x \to \infty$ получаваме (52).

Нека сега $\lambda(n)$ е напълно мултипликативна. За всяко просто число p е изпълнено $|\lambda(p)| < 1$, тъй като в противен случай редът (53) ще е разходящ. От формулата за сума на членовете на безкрайна геометрична прогресия следва

$$T_p = 1 + \lambda(p) + \lambda(p)^2 + \lambda(p)^3 + \cdots = (1 - \lambda(p))^{-1},$$

с което равенството (54) е доказано.

$\square$

3.4 Сравнения

В настоящия параграф ще формулираме понятието „сравнимост на числа по даден модул” и ще докажем негови свойства, необходими за излагането на следващия материал в записките. За по-подробно изучаване на теорията на сравненията препоръчваме на читателя цитираната литература.

Сравнимостта две числа по модул n всъщност представлява равенство в $\mathbb{Z}/n\mathbb{Z}$ на класовете с представители тези числа. Тук обаче ще се придържаме към традиционното изложение, характерно за книги по елементарна теория на числата.

Определение 3.46. *Нека $a, b \in \mathbb{Z}$ и $n \in \mathbb{N}$. Ако $n \mid (a-b)$ казваме, че числата a и b са сравними по модул n и записваме*

$$a \equiv b \pmod{n}.$$

Ако $n \nmid (a-b)$, казваме, че a и b не са сравними по модул n и записваме

$$a \not\equiv b \pmod{n}.$$

Основните свойства на сравненията са изложени в следната

Лема 3.47. *Нека $a, b, c \in \mathbb{Z}$, $k, n \in \mathbb{N}$. Тогава имаме*

(1) $a \equiv a \pmod{n}$.

(2) $a \equiv b \pmod{n} \quad \Longrightarrow \quad b \equiv a \pmod{n}$.

(3) $a \equiv b \pmod{n}, \quad b \equiv c \pmod{n} \quad \Longrightarrow \quad a \equiv c \pmod{n}$.

(4) $a \equiv b \pmod{n}, \quad c \equiv d \pmod{n} \quad \Longrightarrow \quad a \pm c \equiv b \pm d \pmod{n}$.

(4) $a \equiv b \pmod{n}, \quad c \equiv d \pmod{n} \quad \Longrightarrow \quad ac \equiv bd \pmod{n}$.

(5) $a \equiv b \pmod{n} \quad \Longleftrightarrow \quad ak \equiv bk \pmod{nk}$.

(6) $ak \equiv bk \pmod{n}, \quad (n, k) = 1 \quad \Longrightarrow \quad a \equiv b \pmod{n}$.

(7) $a \equiv b \pmod{n}, \quad k \mid n \quad \Longrightarrow \quad a \equiv b \pmod{k}$.

Доказателство. Получава се директно от Определение 3.46 и от свойствата на понятието делимост.

□

Следват определенията на пълна и редуцирана системи от остатъци по даден модул.

Определение 3.48. *Ако $n \in \mathbb{N}$, то всяка система от n на брой цели числа, които са две по две несравними по модул n, се нарича пълна система от остатъци по модул n.*

Например, числата $1, 2, \ldots, n$ образуват пълна система от остатъци по маодул n.

Определение 3.49. *Ако $n \in \mathbb{N}$, то всяка система от $\varphi(n)$ на брой цели числа, които са две по две несравними по модул n и са взаимно прости с n, се нарича редуцирана система от остатъци по модул n.*

Например, естествените числа $k \leq n$, за които $(k, n) = 1$, образуват редуцирана система от остатъци по маодул n.

В следващите леми се дават свойства на системите от остатъци, които по-нататък често ще използваме.

Лема 3.50. *Ако имаме пълна система от остатъци по модул n, то произволно цяло число е сравнимо по модул n с някой неин елемент. Ако пък имаме редуцирана система от остатъци по модул n, то всяко цяло число, което е взаимно просто с n е сравнимо по модул n с число от тази система.*

Доказателство. Следва директно от определенията.

$\square$

Лема 3.51. *Нека $n \in \mathbb{N}$, $h \in \mathbb{Z}$, $(n, h) = 1$. Ако a пробягва пълна (редуцирана) система от остатъци по модул n, то числата ha образуват пълна (редуцирана) система от остатъци по модул n.*

Доказателство. Ако a пробягва пълна система от остатъци по модул n, то според Лема 3.47 (6) числата ha са две по две несравними по модул n. Техният брой е n, следователно образуват пълна система от остатъци по модул n. Разсъжденията са аналогични когато a пробягва редуцирана система от остатъци по модул n.

$\square$

Лема 3.52. *Нека $n_1, n_2 \in \mathbb{N}$, $(n_1, n_2) = 1$. Ако a_1 пробягва пълна (редуцирана) система от остатъци по модул n_1, а a_2 пробягва пълна (редуцирана) система от остатъци по модул n_2, то числата $a_1n_2 + a_2n_1$ образуват пълна (редуцирана) система от остатъци по модул n_1n_2.*

Доказателство. Ако a_1, a_2 пробягват пълни системи от остатъци по модули n_1 и съответно n_2, то числата $a_1n_2 + a_2n_1$ са на брой n_1n_2 и са две по две несравними по модул n_1n_2. Наистина, нека a_1, a_1' са числа от пълна система остатъци по модул n_1 и съответно a_2, a_2' са от пълна система остатъци по модул n_2. Ако

$$a_1n_2 + a_2n_1 \equiv a_1'n_2 + a_2'n_1 \pmod{n_1n_2},$$

то от Лема 3.47 (7), (6) намираме последователно

$$a_1n_2 \equiv a_1'n_2 \pmod{n_1}, \qquad a_1 \equiv a_1' \pmod{n_1}.$$

Аналогично получаваме $a_2 \equiv a_2' \pmod{n_2}$. Оттук следва $a_1 = a_1'$, $a_2 = a_2'$.

По същия начин се разсъждава и когато a_1, a_2 пробягват редуцирани системи от остатъци по модули n_1, n_2, като в този случай използваме още, че функцията на Ойлер $\varphi(n)$ е мултипликативна (виж Лема 3.39).

$\square$

Следва един от основните резултати от елементарната теория на числата.

Теорема 3.53 (Ойлер)**.** *Нека $n \in \mathbb{N}$, $a \in \mathbb{Z}$ и $(a,n)=1$. Тогава е изпълнено*

$$a^{\varphi(n)} \equiv 1 \pmod{n}. \tag{56}$$

Доказателство. Нека $l = \varphi(n)$ и нека $a_1, a_2, \ldots, a_l$ е редуцирама система от остатъци по модул n. Тогава, според Лема 3.51 числата $aa_1, aa_2, \ldots, aa_l$ образуват редуцирана система от остатъци по модул n, откъдето

$$a_1 a_2 \ldots a_l \equiv (aa_1)(aa_2)\ldots(aa_l) \equiv a^l a_1 a_2 \ldots a_l \pmod{n}.$$

Като приложим Лема 3.47 (6) получаваме $a^l \equiv 1 \pmod{n}$, с което лемата е доказана. □

Важен частен случай на Теорема 3.53 е следното твърдение, известно като *малка теорема на Ферма.*

Следствие 3.54 (Ферма)**.** *Ако p е просто число, за което $p \nmid a$, то е изпълнено $a^{p-1} \equiv 1 \pmod{p}$.*

□

При решаването на много задачи от теорията на числата се налага да се изследва сравнение от вида (57), където $f(x)$ е полином с цели коефициенти. Ясно е, че ако някакво число $x_0 \in \mathbb{Z}$ е решение на (57), то всяко $x \in \mathbb{Z}$, за което $x \equiv x_0 \pmod{n}$ също удовлетворява това сравнение и тогава (57) ще има безбройно много решения в цели числа. Естествено е да считаме за идентични решения, принадлежащи на един и същи клас от остатъци по модул n, или все едно, да търсим само решения от някаква фиксирана система от остатъци по модул n. Поради това, въвеждаме следното

Определение 3.55. *Нека $n \in \mathbb{N}$ и $f(x) \in \mathbb{Z}[x]$. Броят на числата x от коя да е пълна система от остатъци по модул n, за които е изпълнено*

$$f(x) \equiv 0 \pmod{n}, \tag{57}$$

се нарича брой на решенията на това сравнение.

Ясно е, че горното определение е коректно, т.е. изборът на конкретна пълна система от остатъци по модул n не влияе върху броя на решенията на (57).

Изследването на броя на решенията на сравнение от вида (57) в общия случай е важна и трудна задача. Тук ще изложим само някои прости резултати, от които ще се нуждаем по-късно.

Лема 3.56. *Нека $n \in \mathbb{N}$, $f \in \mathbb{Z}[x]$ и нека $\beta_f(n)$ означава броя на решенията на сравнението (57). Тогава функцията $\beta_f(n)$ е мултипликативна. Освен това, за всяко $k \in \mathbb{N}$ и за всяко $x \geq 1$ е изпълнено*

$$\sum_{\substack{n \leq x \\ f(n) \equiv 0 \pmod{k}}} 1 = \frac{\beta_f(k)}{k} x + O\left(\beta_f(k)\right), \tag{58}$$

като константата в знака O е абсолютна.

Доказателство. Очевидно $\beta_f(1) = 1$. Нека $n_1, n_2 \in \mathbb{N}$, $(n_1, n_2) = 1$. Според Лема 3.52, ако x_1 пробягва числата $1, 2, \ldots, n_1$, а x_2 съответно $1, 2, \ldots, n_2$, то числата $x_1 n_2 + x_2 n_1$ образуват пълна система от остатъци по модул $n_1 n_2$. По-нататък, сравнението $f(x_1 n_2 + x_2 n_1) \equiv 0 \pmod{n_1 n_2}$ е еквивалентно на системата от две сравнения

$$f(x_1 n_2 + x_2 n_1) \equiv 0 \pmod{n_1}, \qquad f(x_1 n_2 + x_2 n_1) \equiv 0 \pmod{n_2},$$

която пък е еквивалентна на

$$f(x_1 n_2) \equiv 0 \pmod{n_1}, \qquad f(x_2 n_1) \equiv 0 \pmod{n_2}. \tag{59}$$

Тогава

$$\beta_f(n_1 n_2) = \Sigma' \, \Sigma'',$$

където Σ' и Σ'' са съответно броя на числата x_1 измежду $1, 2, \ldots n_1$ и x_2 измежду $1, 2, \ldots n_2$, за които са изпълнени първото, съответно второто от сравненията (59). Според Лема 3.51 числата $x_1 n_2$, където $x_1 = 1, 2, \ldots n_1$ образуват пълна система от остатъци по модул n_1, откъдето $\Sigma' = \beta_f(n_1)$. Аналогично имаме $\Sigma'' = \beta_f(n_2)$. Следователно

$$\beta_f(n_1 n_2) = \beta_f(n_1) \beta_f(n_2),$$

с което мултипликативността на $\beta_f(n)$ е доказана.

Сега ще установим формулата (58). За целта представяме

$$(0, x] = I^* \cup \bigcup_{1 \le l \le \left[\frac{x}{k}\right]} I_l, \qquad \text{където} \qquad I^* = \left(\left[\frac{x}{k}\right] k, x \right], \qquad I_l = ((l-1)k, lk] \, .$$

Целите числа във всеки от интервалите I_l образуват пълна система от остатъци по модул k, следователно всеки от тях съдържа точно $\beta_f(k)$ на брой цели числа m, удовлетворяващи $f(m) \equiv 0 \pmod{k}$. Интервалът I^* е с дължина по-малка от k, следователно броят на целите числа в него, за които е изпълнено същото сравнение, не надхвърля $\beta_f(k)$. Тогава, ако S е сумата в лявата страна на (58), имаме

$$S = \left[\frac{x}{k}\right] \beta_f(k) + \Delta, \qquad 0 \le \Delta \le \beta_f(k).$$

Тогава, като вземем предвид (2), получаваме

$$S = \left(\frac{x}{k} - \left\{ \frac{x}{k} \right\} \right) \beta_f(k) + \Delta = \frac{\beta_f(k)}{k} x + O\left(\beta_f(k)\right),$$

с което лемата е доказана.

□

Следващата лема се отнася до броя на решенията на сравнение от вида (57) с линеен полином $f(x)$.

Лема 3.57. *Нека $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$ и $(a, n) = 1$. Тогава сравнението*

$$ax \equiv b \pmod{n} \tag{60}$$

е разрешимо относно x и има точно едно решение.

Доказателство. Тъй като $(a, n) = 1$, сравнението (60) е еквивалентно на

$$a^{\varphi(n)}x \equiv a^{\varphi(n)-1}b \pmod{n},$$

което пък, според Теорема 3.53, е еквивалентно на

$$x \equiv a^{\varphi(n)-1}b \pmod{n}.$$

□

Следва важно свойство на сравненията от вида (57) в случая когато модулът е просто число.

Лема 3.58. *Нека p е просто число и нека полиномът $f(x) \in \mathbb{Z}[x]$ е от степен m, като поне един от коефициентите му не се дели на p. Тогава сравнението*

$$f(x) \equiv 0 \pmod{p} \tag{61}$$

притежава не повече от m на брой решения.

Доказателство. При $m = 1$ твърдението следва от Лема 3.57. Допускаме, че твърдението е вярно за някое $m \in \mathbb{N}$ и нека $f(x)$ е полином от степен $m+1$, като не всичките му коефициенти са кратни на p. Ако x_0 е решение на (61), представяме дадения полином във вида $f(x) = f(x_0) + (x - x_0)g(x)$, където полиномът $g(x) \in \mathbb{Z}[x]$ е от степен m и не всички от коефициентите му се делят на p. Тогава сравнението (61) е еквивалентно на

$$f(x) \equiv (x - x_0)g(x) \pmod{p} \tag{62}$$

Според индукционното допускане сравнението

$$g(x) \equiv 0 \pmod{p} \tag{63}$$

притежава не повече от m решения. Тъй като p е просто число, всяко решение на (62) ще е сравнимо по модул p с x_0 или с решение на (63). Следователно (61) притежава не повече от $m+1$ решения.

□

Ще отбележим, че ако модулът не е просто число, броят на решенията на сравнението може и да надвишава степента на полинома. Например, сравнението $x^2 \equiv 1 \pmod{8}$ притежава 4 решения.

3.5 Средни стойности на някои аритметични функции

Основна задача в аналитичната теория на числата е намирането на приближена формула за сума от вида

$$\sum_{n \le x} f(n), \tag{64}$$

където $f(n)$ е дадена аритметична функция. В настоящия параграф ще разгледаме случаите, когато $f(n)$ е някоя от функциите $\varphi(n)$, $\sigma(n)$, $\mu^2(n)$. В Глава 4 се изучава сумата (64), когато $f(n)$ е равна на $r(n)$ или на $\tau(n)$. Накрая, в Глава 5 ще се занимаем със средната стойност на функцията на Манголд $\Lambda(n)$, което е в пряка връзка с изучаването на разпределението на простите числа.

Ще започнем с резултат относно средната стойност на функцията на Ойлер.

Лема 3.59. *В сила е асимптотичната формула*

$$\sum_{n\leq x}\varphi(n)=\frac{3}{\pi^2}x^2+O(x\log x). \tag{65}$$

Доказателство. Да означим с S сумата в лявата страна на (65). Като използуваме Лема 3.38, познатата формула $\sum_{j=1}^k j=\frac{k(k+1)}{2}$ и Лема 2.6 (3), получаваме

$$S=\sum_{n\leq x}n\sum_{d\mid n}\frac{\mu(d)}{d}=\sum_{d\leq x}\frac{\mu(d)}{d}\sum_{\substack{n\leq x\\ n\equiv 0 \pmod d}}n=\sum_{d\leq x}\frac{\mu(d)}{d}\sum_{m\leq \frac{x}{d}}md$$

$$=\sum_{d\leq x}\mu(d)\sum_{m\leq\frac{x}{d}}m=\frac{1}{2}\sum_{d\leq x}\mu(d)\left[\frac{x}{d}\right]\left(\left[\frac{x}{d}\right]+1\right)=\frac{1}{2}\sum_{d\leq x}\mu(d)\left(\frac{x^2}{d^2}+O\left(\frac{x}{d}\right)\right)$$

$$=\frac{1}{2}x^2\sum_{d\leq x}\frac{\mu(d)}{d^2}+O\left(x\sum_{d\leq x}\frac{1}{d}\right)=\frac{1}{2}x^2\sum_{d\leq x}\frac{\mu(d)}{d^2}+O\left(x\log x\right). \tag{66}$$

Да означим

$$c=\sum_{d=1}^{\infty}\frac{\mu(d)}{d^2}. \tag{67}$$

От Лема 2.6 (2) следва

$$\sum_{d\leq x}\frac{\mu(d)}{d^2}=c-\sum_{d>x}\frac{\mu(d)}{d^2}=c+O\left(\frac{1}{x}\right). \tag{68}$$

Заместваме получения израз в (66) и виждаме, че

$$S=\frac{c}{2}x^2+O(x\log x). \tag{69}$$

За да намерим стойността на константата c, прилагаме тъждеството на Ойлер (Теорема 3.45) и получаваме

$$c=\prod_p\left(1-\frac{1}{p^2}\right). \tag{70}$$

От друга страна, като използуваме известното равенство $\sum_{n=1}^{\infty}\frac{1}{n^2}=\frac{\pi^2}{6}$ и приложим оже веднъж Теорема 3.45, намираме

$$\frac{\pi^2}{6}=\prod_p\left(1-\frac{1}{p^2}\right)^{-1},$$

следователно

$$c=\frac{6}{\pi^2}. \tag{71}$$

Остава да заместим получената стойност в (69) и получаваме (65).

□

Лема 3.60. *В сила е асимптотичната формула*

$$\sum_{n\le x}\sigma(n)=\frac{\pi^2}{12}x^2+O(x\log x). \tag{72}$$

Доказателство. Разсъжденията са близки до тези в доказателството на предната лема. Подробностите оставяме на читателя.

□

В следващата лема ще разгледаме сумата (64) когато $f(n)$ съвпада с функцията $\mu^2(n)$ и по такъв начин ще получим резултат относно броя на безквадратните числа, ненадминаващи зададена величина.

Лема 3.61. *В сила е асимптотичната формула*

$$\sum_{n\le x}\mu^2(n)=\frac{6}{\pi^2}x+O(\sqrt{x}\,). \tag{73}$$

Доказателство. Да означим с S сумата в лявата страна на (73). Като използуваме тъждеството от Лема 3.44, получаваме

$$S=\sum_{n\le x}\sum_{d^2|n}\mu(d)=\sum_{d\le\sqrt{x}}\mu(d)\sum_{\substack{n\le x\\ n\equiv 0\pmod{d^2}}}1.$$

Но последната сума по n в горната формула очевидно е равна на

$$\left[\frac{x}{d^2}\right]=\frac{x}{d^2}-\left\{\frac{x}{d^2}\right\}$$

(виж формула (2)). Тогава

$$S=\sum_{d\le\sqrt{x}}\mu(d)\left(\frac{x}{d^2}-\left\{\frac{x}{d^2}\right\}\right)=x\sum_{d\le\sqrt{x}}\frac{\mu(d)}{d^2}+O(\sqrt{x}). \tag{74}$$

От формули (68), (71), получени в доказателството на Лема 3.59 имаме

$$\sum_{d\le\sqrt{x}}\frac{\mu(d)}{d^2}=\frac{6}{\pi^2}+O\left(\frac{1}{\sqrt{x}}\right).$$

Оттук и от (74) следва (73).

□

Ще отбележим, че ако вече е получена асимптотична формула за сумата (64), възниква задачата за намиране на възможно най-точна оценка за остатъчния член в тази формула. Обикновено това е трудна задача и за решаването ѝ се налага да бъдат използувани сложни аналитични методи. Например, оценките за остатъчните членове във формулите (65), (72) и (73) могат да бъдат леко усилени, но за това е необходимо да се използуват дълбоки теореми от теорията на дзета-функцията на Риман. Както ще се убедим в Глава 5, тези теореми играят основна роля и при изучаване на средната стойност на функцията на Манголд $\Lambda(n)$. В Глава 4 пък ще видим, че оценките за остатъчните членове в задачите на Гаус и Дирихле могат да бъдат подобрени с помощта на теорията на експоненицалните суми.

Интерес представлява и намирането на приближени формули за суми от вида

$$\sum_{n\le x} f(n)f(n+a)$$

където a е зададено естествено число, а f е аритметична функция. Резултат от такъв тип е представен в следващата теорема. Тя ни дава асимптотична формула за броя на двойките съседни безквадратни числа, ненадминаващи зададено число.

Теорема 3.62. *(Карлиц) При $x \ge 2$ е изпълнено*

$$\sum_{n\le x} \mu^2(n)\mu^2(n+1) = cx + O(x^{\frac{2}{3}+\varepsilon}), \tag{75}$$

където $\varepsilon > 0$ е произволно малко и

$$c = \prod_p \left(1 - \frac{2}{p^2}\right). \tag{76}$$

Доказателство. Означаваме с S сумата в лявата страна на (75). Прилагаме тъждеството от Лема 3.44, след което сменяме реда на сумиране и получаваме

$$S = \sum_{n\le x} \left(\sum_{d^2|n} \mu(d)\right) \left(\sum_{t^2|n+1} \mu(t)\right) = \sum_{\substack{d,t \\ (d,t)=1}} \mu(d)\mu(t)\ F_{d,t}, \tag{77}$$

където

$$F_{d,t} = \#\{n \in \mathbb{N}\ :\ n \le x,\ \ n \equiv 0 \pmod{d^2},\ \ n+1 \equiv 0 \pmod{t^2}\ \}. \tag{78}$$

Да отбележим, че условието $(d,t) = 1$ в последната сума в (77) е следствие на това, че $d^2 \mid n$, $t^2 \mid n+1$ и $(n, n+1) = 1$. Ясно е също така, че d и t удовлетворяват $d \le \sqrt{x}$, $t \le \sqrt{x+1}$, но не е необходимо да поставяме тези условия в областта на сумиране в (77), тъй като ако някое от тях не е изпълнено, то ще имаме $F_{d,t} = 0$.

След като записахме сумата S във вида (77), разделяме я на две части в зависимост от големината на произведението dt. По-точно, нека y е параметър, за който засега предполагаме само, че

$$\sqrt{x} < y < x. \tag{79}$$

(Точната стойност на y ще определим в края на доказателството). Имаме

$$S = S_1 + S_2, \tag{80}$$

където

$$S_1 = \sum_{\substack{dt \le y \\ (d,t)=1}} \mu(d)\mu(t) F_{d,t}, \qquad S_2 = \sum_{\substack{dt > y \\ (d,t)=1}} \mu(d)\mu(t) F_{d,t}. \tag{81}$$

Да разгледдаме първо сумата S_1. За целта записваме величината $F_{d,t}$, определена чрез (78), във вида

$$F_{d,t} = \#\{k \in \mathbb{N} \ : \ k \le x d^{-2}, \ \ kd^2 + 1 \equiv 0 \pmod{t^2} \ \}. \tag{82}$$

Като използуваме, че е налице условието $(d,t) = 1$ и приложим формула (58) от Лема 3.56, получаваме

$$F_{d,t} = \frac{x}{d^2 t^2} + O(1). \tag{83}$$

Оттук и от първата формула в (81) намираме

$$S_1 = \sum_{\substack{dt \le y \\ (d,t)=1}} \mu(d)\mu(t) \left(\frac{x}{d^2 t^2} + O(1) \right) = x\mathcal{G}(y) + O\left(\sum_{dt \le y} 1 \right), \tag{84}$$

където

$$\mathcal{G}(y) = \sum_{\substack{dt \le y \\ (d,t)=1}} \frac{\mu(d)\mu(t)}{d^2 t^2} \tag{85}$$

Но от Определение 3.17, Лема 3.33 и условието (79) виждаме, че

$$\sum_{dt \le y} 1 = \sum_{n \le y} \tau(n) \ll y x^{\varepsilon}, \tag{86}$$

където $\varepsilon > 0$ е произволно малко. Да отбележим, че изразът в дясната страна на (86) може да бъде заменен с $y \log y$ (виж Глава 4), но за нашите цели оценката в настоящия ѝ вид е достатъчно точна.

Сега да разгледаме $\mathcal{G}(y)$. Имаме

$$\mathcal{G}(y) = c - c^*(y), \tag{87}$$

където

$$c = \sum_{\substack{d,t=1 \\ (d,t)=1}}^{\infty} \frac{\mu(d)\mu(t)}{d^2 t^2}, \qquad c^*(y) = \sum_{\substack{dt > y \\ (d,t)=1}} \frac{\mu(d)\mu(t)}{d^2 t^2}. \tag{88}$$

(Очевидно редът, представящ константата c, е абсолютно сходящ).

Ще оценим $c^*(y)$. От Определение 3.17, Лема 3.33 и Лема 2.6 (2) намираме

$$c^*(y) \ll \sum_{dt>y} \frac{1}{d^2t^2} = \sum_{n>y} \frac{\tau(n)}{n^2} \ll \sum_{n>y} \frac{1}{n^{2-\varepsilon}} \ll y^{\varepsilon-1}. \tag{89}$$

Сега, като използваме (79), (84), (86), (87) и (89) получаваме

$$S_1 = x\left(c + O\left(y^{-1}x^{\varepsilon}\right)\right) + O\left(yx^{\varepsilon}\right) = cx + O\left(yx^{\varepsilon}\right).$$

Последната формула, заедно с (80), ни дава

$$S = cx + S_2 + O(yx^{\varepsilon}). \tag{90}$$

Сега ще оценим сумата S_2, определена с (81). Очевидно

$$|S_2| \le \sum_{dt>y} F_{d,t}. \tag{91}$$

Ние разползгаме с формулата (83) за $F_{d,t}$, но нейното използване при оценяването на S_2 не е удачно, тъй като приносът на остатъчния член в (83) към сумата S_2 ще бъде прекалено голям. Поради това ще оценим $F_{d,t}$ по друг начин. Като използваме (82) можем да запишем

$$F_{d,t} = \#\{\langle k, l\rangle \in \mathbb{N}^2 \ : \ kd^2 + 1 = lt^2 \le x + 1\}. \tag{92}$$

От (91) и (92) заключаваме, че

$$|S_2| \le \#\mathcal{H}, \tag{93}$$

където

$$\mathcal{H} = \{\langle d, t, k, l\rangle \in \mathbb{N}^4 \ : \ dt > y, \ \ kd^2 + 1 = lt^2 \le x + 1\}. \tag{94}$$

Разделяме множеството $\mathcal{H}$ на части съобразно порядъците на d и t. По-точно, нека D и T независимо едно от друго пробягват числа от вида 2^j, $j = 0, 1, 2, \dots$ и нека означим

$$\mathcal{W}(D, T) = \{\langle d, t, k, l\rangle \in \mathcal{H} \ : \ D \le d < 2D, \ \ T \le t < 2T\}. \tag{95}$$

Тогава $\mathcal{H}$ се представя като обединение на $O\left(\log^2 x\right)$ множества от вида (95). Ясно е, че за да бъде множеството $\mathcal{W}(D, T)$ непразно е необходимо да са налице условията

$$\frac{1}{2} \le D, T \le \sqrt{x + 1}, \qquad DT \ge \frac{y}{4} \tag{96}$$

Ако означим

$$W(D, T) = \#\mathcal{W}(D, T), \tag{97}$$

то ще имаме

$$\#\mathcal{H} \ll (\log x)^2 \max_{D,T:\,(96)} W(D, T), \tag{98}$$

където максимумът е по всички реални D, T, удовлетворяващи условията (96). Оттук нататък ще считаме, че е изпълнено (96) и ще оценим $W(D,T)$ по два начина.

От (94), (95) и (97) виждаме, че

$$W(D,T) \le \sum_{T \le t < 2T} \sum_{l \le (x+1)T^{-2}} N_{t,l}\,, \tag{99}$$

където

$$N_{t,l} = \#\{\langle d,k\rangle \in \mathbb{N}^2 \ : \ D \le d < 2D, \ \ kd^2 = lt^2 - 1 \le x\}.$$

Ако $l = t = 1$, то очевидно $N_{t,l} = 0$. Нека сега $lt > 1$. От условието $kd^2 = lt^2 - 1$ следва, че $k \mid lt^2 - 1$, т.е. k може да приема най-много $\tau(lt^2 - 1)$ на брой стойности, а при фиксирани k, l, t числото d се определя еднозначно. Тогава, като вземем предвид Лема 3.33, виждаме, че

$$N_{t,l} \le \tau(lt^2 - 1) \ll (lt^2 - 1)^{\varepsilon} \ll x^{\varepsilon}.$$

От горната оценка и от (99) следва

$$W(D,T) \ll x^{1+\varepsilon}\, T^{-1}. \tag{100}$$

От друга страна, с помощта на съображения аналогични на горните, виждаме, че

$$W(D,T) \le \sum_{D \le d < 2D} \sum_{k \le xD^{-2}} M_{d,k}\,, \tag{101}$$

където

$$M_{d,k} = \#\{\langle t,l\rangle \in \mathbb{N}^2 \ : \ T \le t < 2T, \ \ kd^2 + 1 = lt^2 \le x + 1\}.$$

Разсъждавайки както при оценяването на $N_{t,l}$ заключаваме, че

$$M_{d,k} \le \tau(kd^2 + 1) \ll (kd^2 + 1)^{\varepsilon} \ll x^{\varepsilon}$$

и, като използваме (101), получаваме

$$W(D,T) \ll x^{1+\varepsilon}\, D^{-1}. \tag{102}$$

Коя от оценките (100), (102) е по-точна (и, съответно, коя е желателно да използваме) зависи от съотношението между D и T.

Първо да разгледаме случая $T > D$. От второто от условията (96) следва, че $T^2 > DT \ge \frac{y}{4}$, откъдето $T \gg \sqrt{y}$. Тогава, като приложим (100), намираме

$$W(D,T) \ll x^{1+\varepsilon}\, y^{-\frac{1}{2}}. \tag{103}$$

Ако пък е изпълнено $T \le D$, то от (96) следва $D^2 \ge DT \ge \frac{y}{4}$, откъдето $D \gg \sqrt{y}$. Тогава, като приложим (102) виждаме, че оценката (103) отново е налице.

И така, във всички случаи е изпълнено (103). Използуваме (93), (98) и (103) и, след като предефинираме ε, получаваме

$$S_2 \ll x^{1+\varepsilon} y^{-\frac{1}{2}}. \tag{104}$$

От формули (90) и (104) следва

$$S = cx + O\left(x^{\varepsilon} y\right) + O\left(x^{1+\varepsilon} y^{-\frac{1}{2}}\right). \tag{105}$$

Сега ще изберем y по оптимален начин, а именно така че двата остатъчни члена в горната формула да имат еднакъв порядък. Имаме $y = xy^{-\frac{1}{2}}$ точно когато $y = x^{\frac{2}{3}}$. Като заместим тази стойност на y в (105), получаваме асимптотичната формула (75).

Остана да проверим, че константата c, определена чрез (88), удовлетворява (76). Имаме

$$c = \sum_{d=1}^{\infty} \frac{\mu(d)}{d^2} \sum_{t=1}^{\infty} \frac{\mu(t)}{t^2} \chi_d(t), \tag{106}$$

където

$$\chi_d(t) = \begin{cases} 1 & \text{ако} \quad (d,t) = 1, \\ 0 & \text{ако} \quad (d,t) > 1. \end{cases}$$

Очевидно $\frac{\mu(t)}{t^2}\chi_d(t)$ е мултипликативна фукнкция на t, а безкрайният ред по сумационната променлива t в (106) е абсолютно сходящ. Тогава, като приложим тъждеството на Ойлер (Теорема 3.45), намираме

$$\begin{aligned} \sum_{t=1}^{\infty} \frac{\mu(t)}{t^2}\chi_d(t) &= \prod_{p} \left(1 + \frac{\mu(p)}{p^2}\chi_d(p) + \frac{\mu(p^2)}{p^4}\chi_d(p^2) + + \dots\right) \\ &= \prod_{p \nmid d} \left(1 - \frac{1}{p^2}\right) \\ &= \prod_{p} \left(1 - \frac{1}{p^2}\right) \prod_{p \mid d} \left(1 - \frac{1}{p^2}\right)^{-1}. \end{aligned}$$

Заместваме последния израз в (106) и прилагаме отново Теорема 3.45. Получаваме

$$c = \sum_{d=1}^{\infty} \frac{\mu(d)}{d^2} \prod_p \left(1 - \frac{1}{p^2}\right) \prod_{p|d} \left(1 - \frac{1}{p^2}\right)^{-1}$$

$$= \prod_p \left(1 - \frac{1}{p^2}\right) \sum_{d=1}^{\infty} \frac{\mu(d)}{d^2} \prod_{p|d} \left(1 - \frac{1}{p^2}\right)^{-1}$$

$$= \prod_p \left(1 - \frac{1}{p^2}\right) \prod_p \left(1 - \frac{1}{p^2}\left(1 - \frac{1}{p^2}\right)^{-1}\right)$$

$$= \prod_p \left(1 - \frac{2}{p^2}\right).$$

□

Ще отбележим, че оценката за остатъчния член във формулата (75) може да бъде подобрена. С помощта на значително по-сложен метод Хийт-Браун установява, че подазателят $\frac{2}{3}$ може да бъде намален до $\frac{7}{11}$.

3.6 Формули на Якоби за броя на представянията на числата като сума от два и от четири квадрата

В настоящата глава ще илюстрираме теорията разгледана до тук, като докажем класическите формули на Якоби за броя на представянията на числата като суми от два и от четири квадрата. Формула за функцията $r(n)$ от Определение 3.21 е приведена в Теорема 3.66, а Теорема 3.67 се отнася до уравнението на Лагранж

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = n$$

и ни дава формула за броя на неговите решения в цели числа.

За доказателството на Теорема 3.66 ще използуваме един важен резултат относно рационалните приближения на реални числа, известен като *лема на Дирихле*, който играе основна роля при решаването на много задачи от теорията на числата.

Теорема 3.63 (Дирихле). *Нека $\alpha, \tau \in \mathbb{R}, \tau \geq 1$. Съществуват $a \in \mathbb{Z}, q \in \mathbb{N}$, такива че*

$$\left|\alpha - \frac{a}{q}\right| < \frac{1}{q\tau}, \qquad (a, q) = 1, \qquad q \leq \tau. \tag{107}$$

Доказателство. Първо ще намерим $k, m \in \mathbb{Z}$, за които

$$|\alpha m - k| < \tau^{-1}, \qquad 1 \leq m \leq \tau \tag{108}$$

Полагаме $n = [\tau]$ и разглеждаме числата

$$\{\alpha\}, \{2\alpha\}, \dots, \{n\alpha\}. \tag{109}$$

Ако някое от тях, например $s\alpha$, попада в интервала $\left[0, \frac{1}{n+1}\right)$, то получаваме (108) като вземем $m = s, k = [s\alpha]$. Ако пък някое $\{s\alpha\}$ попада в интервала $\left[\frac{n}{n+1}, 1\right)$, то получаваме (108) при $m = s, k = [s\alpha] + 1$.

При $n = 1$ всички възможности са изчерпани. Нека сега $n > 1$ и нека разгледаме случая, когато всички числа (109) попадат в интервала $\left[\frac{1}{n+1}, \frac{n}{n+1}\right)$. Разделяме този интервал на $n - 1$ подинтервала $J_l = \left[\frac{l}{n+1}, \frac{l+1}{n+1}\right)$, $l = 1, 2, \dots, n-1$. Понеже числата (109) са n на брой, то две от тях, например $\{s_1\alpha\}$ и $\{s_2\alpha\}$, където $1 \le s_1 < s_2 \le n$, попадат в един и същи интервал I_l. Следователно

$$|\{s_2\alpha\} - \{s_1\alpha\}| < (n+1)^{-1}.$$

Тогава, като положим $m = s_2 - s_1$, $k = [s_2\alpha] - [s_1\alpha]$ отново получаваме (108).

Сега, като вземем най-големия общ делител $d = (k, m)$ и определим $a = \frac{k}{d}$, $q = \frac{m}{d}$ получаваме числа, удовлетворяващи (107).

$\square$

За доказателството на Теорема 3.66 са ни нужни още две помощни твърдения.

Лема 3.64. *Ако $n \in \mathbb{N}$, $n > 1$, то броят на наредените двойки $\langle x, y\rangle \in \mathbb{N}^2$, за които*

$$x^2 + y^2 = n, \qquad (x, y) = 1 \tag{110}$$

е равен на броя на решенията на сравнението

$$z^2 + 1 \equiv 0 \pmod{n}. \tag{111}$$

Доказателство. Нека $\mathcal{X}$ е множеството от наредени двойки $\langle x, y\rangle \in \mathbb{N}^2$ удовлетворяващи (110). Означаваме с $\mathcal{Y}$ множеството от решенията на сравнението (111), т.е. съвокупността от класовете от остатъци по модул n, представителите на които удовлетворяват (111). Ще определим изображение

$$\sigma : \mathcal{X} \to \mathcal{Y} \tag{112}$$

и ще докажем, че то е биекция между тези множества.

Нека $\langle x, y\rangle \in \mathcal{X}$. От (110) следва, че $(n, y) = 1$. Според Лема 3.57 съществува единствен клас от остатъци z по модул n такъв, че

$$x \equiv zy \pmod{n}. \tag{113}$$

За него имаме

$$(z^2 + 1)y^2 \equiv (zy)^2 + y^2 \equiv x^2 + y^2 \equiv 0 \pmod{n}.$$

От последната формула, от условието $(n, y) = 1$ и от Лема 3.47 (6) получаваме $z^2 + 1 \equiv 0 \pmod{n}$, а това означава, че $z \in \mathcal{Y}$. Определяме изображенито (112), като на $\langle x, y\rangle \in \mathcal{X}$ съпоставим елемента $z \in \mathcal{Y}$.

Първо ще докажем, че σ е инективно. Нека

$$\langle x, y\rangle, \langle x', y'\rangle \in \mathcal{X}, \qquad \langle x, y\rangle \neq \langle x', y'\rangle$$

и да допуснем, че образите на тези два елемента при σ съвпадат, т.е. съществува $z \in \mathcal{Y}$ такова, че

$$x \equiv zy \pmod{n}, \qquad x' \equiv zy' \pmod{n}.$$

От тези сравнения намираме

$$xy' - yx' \equiv 0 \pmod{n}. \tag{114}$$

Но от това, че числата x, y удовлетворяват уравнението в (110) и от условието $n > 1$ получаваме $0 < x, x', y, y' < \sqrt{n}$, откъдето $0 < xy', yx' < n$. Следователно

$$-n < xy' - yx' < n,$$

което, заедно с (114), ни дава

$$xy' - yx' = 0.$$

От горното равенство и от условията $(x, y) = (x', y') = 1$ следва $x = x'$, $y = y'$ (елементарната проверка оставяме на читателя). Последното, обаче, е в противаречие с нашето допускане, че двойките $\langle x, y\rangle$ и $\langle x', y'\rangle$ са различни. С това инективността на σ е доказана.

Сега ще докажем, че σ е сюрективно. Да вземем произволно $z \in \mathcal{Y}$. Можем да считаме, че $z \in \mathbb{Z}$, т.е. отъждествяваме класа от остатъци по модул n с някакъв негов представител от $\mathbb{Z}$. Прилагаме лемата на Дирихле (Теорема 3.63) при $\alpha = \frac{z}{n}$, $\tau = \sqrt{n}$ и заключаваме, че съществуват $a, q \in \mathbb{Z}$, удовлетворяващи

$$\left|\frac{z}{n} - \frac{a}{q}\right| < \frac{1}{q\sqrt{n}}, \qquad 1 \leq q \leq \sqrt{n}, \qquad (a, q) = 1. \tag{115}$$

Сега, ако положим

$$r = zq - an, \tag{116}$$

то имаме

$$|r| < \sqrt{n}. \tag{117}$$

Оттук получаваме

$$r^2 + q^2 = (zq - an)^2 + q^2 = z^2q^2 - 2zqan + a^2n^2 + q^2 \equiv (z^2 + 1)q^2 \pmod{n}.$$

Но z удовлетворява (111), следователно

$$r^2 + q^2 \equiv 0 \pmod{n}. \tag{118}$$

От неравенствата за q в (115) и от оценката (117) следва

$$0 < r^2 + q^2 < 2n$$

и, като вземем предвид (118), получаваме

$$r^2 + q^2 = n. \tag{119}$$

Сега ще проверим, че

$$(r, q) = 1. \tag{120}$$

От равенствата (116) и (119) получаваме

$$n = (zq - an)^2 + q^2 = (zq - an)zq - (zq - an)an + q^2 = (zq - an)zq - ran + q^2,$$

а оттук следва

$$(ra + 1)n = \big((z^2 + 1)q - anz\big)\, q.$$

Като разделим последното равенство с n и положим

$$k = \frac{z^2 + 1}{n}\, q - az$$

намираме

$$ra + 1 = kq. \tag{121}$$

Но от условието (111) виждаме, че $k \in \mathbb{Z}$, а оттук и от (121) следва (120).

От (120) заключаваме, че $r \neq 0$. Наистина, в противен случай от (120) би следвало, че $q = 1$ и, като вземем предвид (119), ще имаме $n = 1$, а това противоречи на условието на лемата.

Да разгледаме случая $r > 0$. Като положим

$$x = r, \qquad y = q \tag{122}$$

намираме наредена двойка $\langle x, y \rangle \in \mathbb{N}^2$, която, вследствие на (119) и (120) удовлетворява условията (110), следователно $\langle x, y \rangle \in \mathcal{X}$. От друга страна, от (116) и (122) виждаме, че е изпълнено (113) и това означава, че z е образ на $\langle x, y \rangle$ при изображението σ.

Нека сега $r < 0$. В този случай полагаме

$$x = q, \qquad y = -r \tag{123}$$

и, като използуваме (119) и (120), виждаме, че отново са изпълнени условията (110), следователно $\langle x, y \rangle \in \mathcal{X}$. От (116) и (123) следва $-y \equiv zx \pmod{n}$. От последното сравнение и от условието, че z удовлетворява (111) получаваме

$$-zy \equiv z^2 x \equiv -x \pmod{n}.$$

Тогава е налице (113), следователно z е образ на $\langle x, y \rangle$ при изображението σ.

С това сюрективността на σ е установена и лемата е доказана.

□

В следващата лема се дава информация за броя на решенията на

$$x^2 + 1 \equiv 0 \pmod{n}, \tag{124}$$

в случая когато n е степен на просто число.

Лема 3.65. *Ако $\beta(n)$ е броя на решенията на сравнението* (124)*, то за произволно просто p и за всяко $l \in \mathbb{N}$ е изпълнено*

$$\beta\left(p^l\right) = \begin{cases} 2 & \text{ако} \quad p \equiv 1 \pmod 4, \\ 0 & \text{ако} \quad p \equiv 3 \pmod 4, \\ 1 & \text{ако} \quad p = 2, \quad l = 1, \\ 0 & \text{ако} \quad p = 2, \quad l \geq 2. \end{cases} \tag{125}$$

Доказателство. Очевидно е, че $\beta(2) = 1$.

При $l \geq 2$ всяко решение на сравнението $x^2 + 1 \equiv 0 \pmod{2^l}$ удовлетворява и $x^2 + 1 \equiv 0 \pmod 4$, а както непосредствено се проверява, последното няма решение. Оттук следва, че $\beta(2^l) = 0$ при $l \geq 2$.

Нека $p \equiv 3 \pmod 4$. Ще проверим, че $\beta(p) = 0$, откъдето непосредствено следва, че $\beta(p^l) = 0$ за всяко $l \in \mathbb{N}$. Наистина, нека допуснем, че за някое $x_0 \in \mathbb{Z}$ имаме $x_0^2 + 1 \equiv 0 \pmod p$. Очевидно $p \nmid x_0$ и тогава, като използуваме малката теорема на Ферма (Следствие 3.54), получаваме

$$-1 = (-1)^{\frac{p-1}{2}} \equiv (x_0^2)^{\frac{p-1}{2}} = x_0^{p-1} \equiv 1 \pmod p,$$

което е невъзможно.

Остана да разгледаме случая $p \equiv 1 \pmod 4$ и да докажем, че за всяко $l \in \mathbb{N}$ имаме

$$\beta(p^l) = 2. \tag{126}$$

Нека първо $l = 1$. Ясно е, че ако x_0 е решение на

$$x^2 + 1 \equiv 0 \pmod p, \tag{127}$$

то $-x_0$ също е решение, и то несравнимо по модул p с първото. Тогава, като вземем предвид Лема 3.58 виждаме, че ако докажем разрешимостта на (127), то получаваме равенството

$$\beta(p) = 2. \tag{128}$$

От малката теорема на Ферма (Следствие 3.54) виждаме, че сравнението $x^{p-1} \equiv 1 \pmod p$ притежава точно $p - 1$ на брой решения. Очевидно е, че това сравнение е еквивалентно на

$$\left(x^{\frac{p-1}{2}} - 1\right)\left(x^{\frac{p-1}{2}} + 1\right) \equiv 0 \pmod p.$$

Тъй като $p > 2$, то всяко x, за което $p \nmid x$ е решение на точно едно от сравненията

$$x^{\frac{p-1}{2}} - 1 \equiv 0 \pmod p, \qquad x^{\frac{p-1}{2}} + 1 \equiv 0 \pmod p. \tag{129}$$

От равенството $(-1)^{\frac{p-1}{2}} + 1 = 2$ следва, че числото -1 не е решение на второто от тях, следователно е решение на първото. Но числата

$$1^2, 2^2, 3^2, \ldots, \left(\frac{p-1}{2}\right)^2 \tag{130}$$

са две по две несравними по модул p (простата проверка оставяме на читателя) и, според Следствие 3.54, всяко от тях е решение на първото от сравненията (129). От друга страна, от Лема 3.58 знаем, че същото сравнение не може да има повече от $\frac{p-1}{2}$ на брой решения, следователно всяко негово решение е сравнимо по модул p с някое от числата (130). В частност, числото -1 е сравнимо с някое от тези числа, което означава, че сравнението (127) има решение. С това равенството (128) е доказано.

Сега ще докажем, че за всяко $l \in \mathbb{N}$ имаме

$$\beta(p^l) = \beta(p^{l+1}). \tag{131}$$

От (128) и (131) следва, че (126) е вярно за всяко $l \in \mathbb{N}$ и лемата ще бъде доказана.

За да докажем (131) е достатъчно да установим, че ако x_0 е решение на

$$x^2 + 1 \equiv 0 \pmod{p^l}, \tag{132}$$

то в произволна пълна система от остатъци по модул p^{l+1} съществува единствено x_1, което удовлетворява

$$x_1^2 + 1 \equiv 0 \pmod{p^{l+1}}, \qquad x_1 \equiv x_0 \pmod{p^l}. \tag{133}$$

Търсим x_1 във вида $x_1 = x_0 + mp^l$, където $m \in \mathbb{Z}$. Тогава второто условие в (133) е изпълнено. За да удовлетворим и първото условие ще изберем по подходящ начин числото m. Имаме

$$x_1^2 + 1 = \left(x_0 + mp^l\right)^2 + 1 = x_0^2 + 2x_0mp^l + m^2p^{2l} + 1 \equiv x_0^2 + 1 + 2x_0mp^l \pmod{p^{l+1}}.$$

Тъй като x_0 е решение на (132), то от горната формула следва, че първото от условията (133) е еквивалентно на

$$\frac{x_0^2 + 1}{p^l} + 2x_0m \equiv 0 \pmod{p}. \tag{134}$$

Очевидно е, че $p \nmid 2x_0$, следователно, според Лема 3.57, съществува единствено m по модул p, за което да е налице (134). Тогава в произволна пълна система от остатъци по модул p^{l+1} съществува единствено x_1, удовлетворяващо (133). С това лемата е доказана.

□

Вече сме готови за извеждането на точната формула за функцията $r(n)$ от Определение 3.21.

Теорема 3.66 (Якоби)**.** *При произволно $n \in \mathbb{N}$ е изпълнено*

$$r(n) = 4\sum_{d|n} \chi(d), \tag{135}$$

където

$$\chi(d) = \begin{cases} 1 & \text{ако} \quad d \equiv 1 \pmod{4}, \\ -1 & \text{ако} \quad d \equiv 3 \pmod{4}, \\ 0 & \text{ако} \quad d \equiv 0 \pmod{2}. \end{cases} \tag{136}$$

Доказателство. При $n = 1$ равенството (135) се проверява непосредствено и отсега нататък ще считаме, че $n > 1$.

Ако са налице условията

$$x^2 + y^2 = n, \qquad (x, y) = d, \tag{137}$$

то $d^2 \mid n$ и поради това имаме

$$r(n) = \sum_{x^2+y^2=n} 1 = \sum_{d^2|n} \sum_{\substack{x^2+y^2=n \\ (x,y)=d}} 1 = \sum_{\substack{d^2|n \\ d^2<n}} \sum_{\substack{x^2+y^2=n \\ (x,y)=d}} 1 + \delta_n,$$

където

$$\delta_n = \begin{cases} 4 & \text{ако } n \text{ е точен квадрат,} \\ 0 & \text{в противен случай.} \end{cases} \tag{138}$$

Ако x, y удовлетворяват (137), то можем да ги представим във вида $x = dx_1$, $y = dy_1$, където

$$x_1^2 + y_1^2 = \frac{n}{d^2}, \qquad (x_1, y_1) = 1. \tag{139}$$

Но ако $d^2 < n$, то на всяка наредена двойка $\langle x_1, y_1 \rangle \in \mathbb{N}^2$, за която е изпълнено (139) съответсват точно 4 наредени двойки $\langle x_1, y_1 \rangle \in \mathbb{Z}^2$, удовлетворяващи (139), а именно $\langle \pm x_1, \pm y_1 \rangle$. От тези съображения и от Лема 3.64 получаваме

$$r(n) = \sum_{\substack{d^2|n \\ d^2<n}} \sum_{\substack{x_1^2+y_1^2=\frac{n}{d^2} \\ (x_1,y_1)=1}} 1 + \delta_n = 4 \sum_{\substack{d^2|n \\ d^2<n}} \sum_{\substack{x_1^2+y_1^2=\frac{n}{d^2} \\ (x_1,y_1)=1 \\ x_1, y_1>0}} 1 + \delta_n$$

$$= 4 \sum_{\substack{d^2|n \\ d^2<n}} \beta\left(\frac{n}{d^2}\right) + \delta_n,$$

където $\beta(n)$ е броя на решенията на сравнението (124). Тогава от (138) виждаме, че последната формула може да бъде записана във вида

$$r(n) = 4F(n), \qquad \text{където} \qquad F(n) = \sum_{d^2|n} \beta\left(\frac{n}{d^2}\right). \tag{140}$$

Да положим

$$G(n) = \sum_{d|n} \chi(d). \tag{141}$$

От (140) и (141) виждаме, че за да докажем тъждеството (135) е достатъчно да установим, че при $n > 1$ е изпълнено

$$F(n) = G(n). \tag{142}$$

Лесно се проверява, че функцията $\chi(d)$, определена чрез (136), е напълно мултипликативна и тогава от Следствие 3.31 виждаме, че $G(n)$ е мултипликативна. От друга страна, функцията $F(n)$ може да бъде записана във вида

$$F(n) = \sum_{d|n} \beta\left(\frac{n}{d}\right)\lambda(d), \qquad \text{където} \qquad \lambda(d) = \begin{cases} 1 & \text{ако } d \text{ е точен квадрат,} \\ 0 & \text{в противен случай.} \end{cases}$$

Според Лема 3.56 функцията $\beta(n)$ е мултипликативна, а мултипликативността на $\lambda(n)$ е очевидна. Тогава от Лема 3.30 следва, че и $F(n)$ е мултипликативна. Следователно, като вземем предвид Лема 3.27 виждаме, че за да установим тъждеството (142) е достатъчно да проверим, че

$$F\left(p^l\right) = G\left(p^l\right) \qquad \text{ако } p \text{ е просто и } l \in \mathbb{N}. \tag{143}$$

За да докажем горното равенство първо ще отбележим, че от (140) следва

$$F\left(p^l\right) = \sum_{d^2|p^l} \beta\left(\frac{p^l}{d^2}\right) = \sum_{0\le v\le \frac{l}{2}} \beta\left(p^{l-2v}\right)$$

$$= \begin{cases} \beta\left(p^l\right) + \beta\left(p^{l-2}\right) + \cdots + \beta\left(p^4\right) + \beta\left(p^2\right) + \beta(1) & \text{ако} \quad 2 \mid l, \\ \\ \beta\left(p^l\right) + \beta\left(p^{l-2}\right) + \cdots + \beta\left(p^5\right) + \beta\left(p^3\right) + \beta\left(p\right) & \text{ако} \quad 2 \nmid l. \end{cases} \tag{144}$$

Съответно, като използуваме (141) намираме

$$G(p^l) = 1 + \chi\left(p\right) + \chi\left(p\right)^2 + \cdots + \chi\left(p\right)^l. \tag{145}$$

Ще разгледаме три случая.

1) Нека $p = 2$.

От (136) и (145) следва

$$G\left(2^l\right) = 1,$$

а от (144) и от Лема 3.65 имаме

$$F\left(2^l\right) = \begin{cases} \beta(1) & \text{ако} \quad 2 \mid l, \\ \\ \beta\left(2\right) & \text{ако} \quad 2 \nmid l \end{cases}$$

$$= 1.$$

И така, в настоящия случай равенството (143) е изпълнено.

2) Нека $p \equiv 1 \pmod 4$.

Като използуваме (136) и (145) получаваме

$$G\left(p^l\right) = l + 1.$$

От друга страна, от (144) и Лема 3.65 намираме

$$F\left(p^l\right) = \begin{cases} \underbrace{2 + 2 + \cdots + 2}_{l/2 \text{ пъти}} + 1 & \text{ако} \quad 2 \mid l, \\ \\ \underbrace{2 + 2 + \cdots + 2}_{(l+1)/2 \text{ пъти}} & \text{ако} \quad 2 \nmid l \end{cases}$$

$$= l + 1.$$

С това проверихме верността на (143) и във втория случай.

3) Нека $p \equiv 3 \pmod 4$.

Отново използуваме (136) и (145) и получаваме

$$G\left(p^l\right) = 1 - 1 + 1 - \cdots + (-1)^l$$

$$= \begin{cases} 1 & \text{ако} \quad 2 \mid l, \\ 0 & \text{ако} \quad 2 \nmid l. \end{cases}$$

Съответно, от (144) и Лема 3.65 намираме

$$F\left(p^l\right) = \begin{cases} 1 & \text{ако} \quad 2 \mid l, \\ 0 & \text{ако} \quad 2 \nmid l. \end{cases}$$

Или равенството (143) е изпълнено и в третия случай.

С това доказателството на (142) е завършено и теоремата е доказана.

□

Сега, като използваме Теорема 3.66, ще получим формулата на Якоби за броя на решенията на уравнението на Лагранж

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = n. \tag{146}$$

Изложеното доказателство е получено от Спиърмън и Уилямс и е напълно елементарно. Ще отбележим, че съществуват и по-кратки доказателства на тази забележителна теорема.

Теорема 3.67 (Якоби)**.** *За всяко $n \in \mathbb{N}$ означаваме с $R(n)$ броя на решенията на уравнението* (146) *в числа $x_1, x_2, x_3, x_4 \in \mathbb{Z}$. Тогава е в сила равенството*

$$R(n) = 8 \sum_{\substack{d \mid n \\ d \not\equiv 0 \pmod 4}} d. \tag{147}$$

Доказателство. При $n = 1, 2$ равенството (147) се проверява непосредствено. Оттук нататък ще считаме, че $n > 2$.

Като използуваме Определение 3.21 записваме

$$R(n) = \sum_{x_1^2+x_2^2+x_3^2+x_4^2=n} 1 = \sum_{k=0}^{n} \left(\sum_{x_1^2+x_2^2=k} 1 \right) \left(\sum_{x_1^2+x_2^2=n-k} 1 \right) = \sum_{k=0}^{n} r(k)\, r(n-k).$$

В последната сума отделяме събираемите, за които $k = 0$ и $k = n$, след което използуваме Теорема 3.66. Получаваме

$$\begin{aligned} R(n) &= 2r(0)r(n) + \sum_{k=1}^{n-1} r(k)\, r(n-k) \\ &= 8 \sum_{d|n} \chi(d) + 16\mathcal{F}(n), \end{aligned} \tag{148}$$

където

$$\mathcal{F}(n) = \sum_{k=1}^{n-1} \left(\sum_{d|k} \chi(d) \right) \left(\sum_{t|n-k} \chi(t) \right).$$

Да разгледаме $\mathcal{F}(n)$. Като сменим реда на сумиране, получаваме

$$\begin{aligned} \mathcal{F}(n) &= \sum_{d,t} \chi(d)\chi(t) \sum_{\substack{1\le k\le n-1 \\ k\equiv 0 \pmod d \\ n-k\equiv 0 \pmod t}} 1 \\ &= \sum_{d,t} \chi(d)\chi(t) \sum_{\substack{k+l=n \\ k\equiv 0 \pmod d \\ l\equiv 0 \pmod t}} 1 \\ &= \sum_{dD+tT=n} \chi(d)\chi(t). \end{aligned}$$

(Сумирането се извършва по четворките естествени числа d, D, t, T, удовлетворяващи съответното уравнение).

Като използуваме (136) виждаме, че

$$\chi(d)\chi(t) = \begin{cases} 1 & \text{ако} \quad d \equiv t \equiv 1 \pmod 2 \quad \text{и} \quad d \equiv t \pmod 4, \\ -1 & \text{ако} \quad d \equiv t \equiv 1 \pmod 2 \quad \text{и} \quad d \equiv -t \pmod 4, \\ 0 & \text{в останалите случаи.} \end{cases}$$

Следователно

$$\mathcal{F}(n) = \mathcal{F}_1 - \mathcal{F}_2, \tag{149}$$

където
$$\mathcal{F}_1 = \sum_{\substack{dD+tT=n \\ d\equiv t\equiv 1 \pmod 2 \\ d\equiv t \pmod 4}} 1, \qquad \mathcal{F}_2 = \sum_{\substack{dD+tT=n \\ d\equiv t\equiv 1 \pmod 2 \\ d\equiv -t \pmod 4}} 1.$$
От горните формули лесно се вижда, че
$$\mathcal{F}_1 = \mathcal{G}_1 - \mathcal{G}', \qquad \mathcal{F}_2 = \mathcal{G}_2 - \mathcal{G}', \tag{150}$$
където
$$\mathcal{G}_1 = \sum_{\substack{dD+tT=n \\ d\equiv t \pmod 4}} 1, \qquad \mathcal{G}_2 = \sum_{\substack{dD+tT=n \\ d\equiv -t \pmod 4}} 1, \qquad \mathcal{G}' = \sum_{\substack{dD+tT=n \\ d\equiv t\equiv 0 \pmod 2 \\ d\equiv t \pmod 4}} 1. \tag{151}$$
От (149) и (150) следва
$$\mathcal{F}(n) = \mathcal{G}_1 - \mathcal{G}_2. \tag{152}$$

Да разгледаме $\mathcal{G}_1$. Имаме
$$\mathcal{G}_1 = \mathcal{G}_1' + \mathcal{G}_1'' + \mathcal{G}_1^*, \tag{153}$$
където $\mathcal{G}_1'$ и $\mathcal{G}_1''$ съдържат събираемите от $\mathcal{G}_1$, за които $d > t$ и съответно $d < t$, а $\mathcal{G}_1^*$ е приносът на събираемите, за които $d = t$.

Да намерим първо формула за $\mathcal{G}_1^*$. Ако $d = t$ и е изпълнено $dD + tT = n$, то $d \mid n$ и тогава имаме
$$\mathcal{G}_1^* = \sum_{d|n} \sum_{D+T=\frac{n}{d}} 1 = \sum_{d|n} \left(\frac{n}{d} - 1\right).$$
Тогава, като използваме Определения 3.17, 3.18 и факта, че ако d пробягва делителите на n, то $\frac{n}{d}$ също пробягва делителите на n, получаваме
$$\mathcal{G}_1^* = \sigma(n) - \tau(n). \tag{154}$$

По-нататък, очевидно имаме
$$\mathcal{G}_1' = \mathcal{G}_1'' = \sum_{\substack{dD+tT=n \\ d=t+4k \text{ за някое } k\in\mathbb{N}}} 1 = \sum_{(t+4k)D+tT=n} 1 = \sum_{4kD+t(D+T)=n} 1 = \sum_{\substack{4kD+tE=n \\ D<E}} 1. \tag{155}$$
(Сумационните променливи в последната сума са естествени числа).

Сега да разгледаме израза $\mathcal{G}_2$, определен от (151). Имаме
$$\mathcal{G}_2 = \mathcal{G}_2' + \mathcal{G}_2'' + \mathcal{G}_2^*, \tag{156}$$
където $\mathcal{G}_2'$ и $\mathcal{G}_2''$ съдържат събираемите от $\mathcal{G}_2$, за които $D > T$ и съответно $D < T$, а $\mathcal{G}_2^*$ е приносът на събираемите, за които $D = T$.

Ясно е, че

$$\mathcal{G}_2^* = \sum_{\substack{D(d+t)=n \\ d+t\equiv 0 \pmod 4}} 1 = \sum_{\substack{Dl=n \\ l\equiv 0 \pmod 4}} \sum_{d+t=l} 1 = \sum_{h|\frac{n}{4}} \sum_{d+t=4h} 1 = \sum_{h|\frac{n}{4}} (4h-1).$$

Да отбележим, че горната сума е празна при $4 \nmid n$. За опростяване на записа оттук нататък ще считаме, че

$$\sigma(\varkappa) = \tau(\varkappa) = 0 \qquad \text{ако} \qquad \varkappa \notin \mathbb{N} \tag{157}$$

и тогава можем да запишем

$$\mathcal{G}_2^* = 4\sigma\left(\frac{n}{4}\right) - \tau\left(\frac{n}{4}\right). \tag{158}$$

По-нататък, имаме

$$\mathcal{G}_2' = \mathcal{G}_2'' = \sum_{\substack{dD+tT=n \\ d+t\equiv 0 \pmod 4 \\ D<T}} 1 = \sum_{\substack{dD+t(D+E)=n \\ d+t\equiv 0 \pmod 4}} 1 = \sum_{\substack{(d+t)D+tE=n \\ d+t\equiv 0 \pmod 4}} 1 = \sum_{\substack{4hD+tE=n \\ 4h>t}} 1. \tag{159}$$

От (152) – (159) получаваме

$$\mathcal{F}(n) = 2(\mathcal{A}_1 - \mathcal{B}_1) + \sigma(n) - \tau(n) - 4\sigma\left(\frac{n}{4}\right) + \tau\left(\frac{n}{4}\right), \tag{160}$$

където

$$\mathcal{A}_1 = \sum_{\substack{4hD+tE=n \\ D<E}} 1, \qquad \mathcal{B}_1 = \sum_{\substack{4hD+tE=n \\ 4h>t}} 1. \tag{161}$$

Полагаме също

$$\mathcal{A}_2 = \sum_{\substack{4hD+tE=n \\ D>E}} 1, \qquad \mathcal{B}_2 = \sum_{\substack{4hD+tE=n \\ 4h<t}} 1, \tag{162}$$

$$\mathcal{A}_3 = \sum_{\substack{4hD+tE=n \\ D=E}} 1, \qquad \mathcal{B}_3 = \sum_{\substack{4hD+tE=n \\ 4h=t}} 1. \tag{163}$$

От (161) – (163) получаваме

$$\mathcal{A}_1 + \mathcal{A}_2 + \mathcal{A}_3 = \sum_{4hD+tE=n} 1 = \mathcal{B}_1 + \mathcal{B}_2 + \mathcal{B}_3.$$

Имаме също така

$$\mathcal{A}_2 = \sum_{4h(E+H)+tE=n} 1 = \sum_{4hH+(4h+t)E=n} 1 = \sum_{\substack{4hH+lE=n \\ 4h<l}} 1 = \mathcal{B}_2.$$

От последните формули следва $\mathcal{A}_1 + \mathcal{A}_3 = \mathcal{B}_1 + \mathcal{B}_3$, откъдето $\mathcal{A}_1 - \mathcal{B}_1 = \mathcal{B}_3 - \mathcal{A}_3$. Тогава, като вземем предвид (160), получаваме

$$\mathcal{F}(n) = 2(\mathcal{B}_3 - \mathcal{A}_3) + \sigma(n) - \tau(n) - 4\sigma\left(\frac{n}{4}\right) + \tau\left(\frac{n}{4}\right). \tag{164}$$

Остава да изчислим $\mathcal{A}_3$ и $\mathcal{B}_3$. Имаме

$$\mathcal{A}_3 = \sum_{(4h+t)D=n} 1 = \sum_{D|n} \sum_{4h+t=\frac{n}{D}} 1 = \sum_{D|n} \sum_{4h+t=D} 1 = \sum_{D|n} \sum_{\substack{t \le D-1 \\ t \equiv D \pmod 4}} 1.$$

Ще използуваме, че за $x \in \mathbb{R}$, $x \ge 0$ и за $q \in \mathbb{N}, v \in \mathbb{Z}$ е в сила равенството

$$\sum_{\substack{k \le x \\ k \equiv v \pmod q}} 1 = \left[\frac{x-v}{q}\right] - \left[\frac{-v}{q}\right].$$

(Простата проверка оставяме на читателя). Тогава получаваме

$$\mathcal{A}_3 = \sum_{D|n} \left(\left[\frac{-1}{4}\right] - \left[\frac{-D}{4}\right]\right) = \sum_{D|n} \left(-1 - \left[\frac{-D}{4}\right]\right) = -\tau(n) - \sum_{D|n} \left[\frac{-D}{4}\right]. \tag{165}$$

Разделяме сумата по D на части, съобразно остатъка на D по модул 4 и използуваме, че при $D \equiv j \pmod 4$ е изпълнено

$$\left[\frac{-D}{4}\right] = \begin{cases} -\frac{1}{4}D & \text{ако} \quad j = 0, \\ -\frac{1}{4}(D-j) - 1 & \text{ако} \quad j = 1, 2, 3. \end{cases} \tag{166}$$

Тогава, ако въведем означението

$$\tau_j(n) = \sum_{\substack{d|n \\ d \equiv j \pmod 4}} 1\,, \qquad j = 0, 1, 2, 3, \tag{167}$$

и използуваме очевидните равенства

$$\sigma(n) = \sum_{j=0}^{3} \sum_{\substack{d|n \\ d \equiv j \pmod 4}} d, \qquad \tau(n) = \sum_{j=0}^{3} \tau_j(n) \tag{168}$$

получаваме

$$\mathcal{A}_3 = -\tau(n) + \frac{1}{4} \sum_{\substack{D|n \\ D \equiv 0 \pmod 4}} D \; + \sum_{j=1}^{3} \sum_{\substack{D|n \\ D \equiv j \pmod 4}} \left(\frac{D-j}{4} + 1\right)$$

$$= -\tau(n) + \frac{1}{4}\sigma(n) - \sum_{j=1}^{3} \sum_{\substack{D|n \\ D \equiv j \pmod 4}} \left(\frac{j}{4} - 1\right)$$

$$= \frac{1}{4}\sigma(n) - \tau_0(n) - \frac{1}{4}\tau_1(n) - \frac{1}{2}\tau_2(n) - \frac{3}{4}\tau_3(n). \tag{169}$$

Сега да разгледаме израза $\mathcal{B}_3$, определен от (163). Като използваме означението (157) получаваме

$$\mathcal{B}_3 = \sum_{4h(D+E)=n} 1 = \sum_{h|\frac{n}{4}} \sum_{D+E=\frac{n}{4h}} 1 = \sum_{h|\frac{n}{4}} \sum_{D+E=h} 1 = \sum_{h|\frac{n}{4}} (h-1) = \sigma\left(\frac{n}{4}\right) - \tau\left(\frac{n}{4}\right).$$

От последната формула, (164), (168) и (169) следва

$$\begin{aligned}\mathcal{F}(n) &= 2\left(\sigma\left(\frac{n}{4}\right) - \tau\left(\frac{n}{4}\right) - \frac{1}{4}\sigma(n) + \tau_0(n) + \frac{1}{4}\tau_1(n) + \frac{1}{2}\tau_2(n) + \frac{3}{4}\tau_3(n)\right) \\ &\quad + \sigma(n) - 4\sigma\left(\frac{n}{4}\right) - \tau(n) + \tau\left(\frac{n}{4}\right) \\ &= \frac{1}{2}\sigma(n) - 2\sigma\left(\frac{n}{4}\right) - \frac{1}{2}\tau_1(n) + \frac{1}{2}\tau_3(n). \end{aligned} \tag{170}$$

Получената формула за $\mathcal{F}(n)$ заместваме в (148). По-нататък, от определението (136) за $\chi(d)$ и от означението (167) следва

$$\sum_{d|n} \chi(d) = \tau_1(n) - \tau_3(n). \tag{171}$$

Тогава от (148), (170) и (171) получаваме

$$R(n) = 8\left(\sigma(n) - 4\sigma\left(\frac{n}{4}\right)\right) = 8 \sum_{\substack{d|n \\ d\not\equiv 0 \pmod 4}} d.$$

С това теоремата е доказана.

$\square$

Следствие 3.68 (Теорема на Лагранж)**.** *Всяко естествено число може да се представи като сума от четири квадрата на цели числа.*

Доказателство. Сумата в дясната страна на (147) съдържа събираемо, отговарящо на $d = 1$. Следователно $R(n) \geq 8$ за всяко $n \in \mathbb{N}$.

$\square$

4 Задачите за броя на целите точки в кръга и под хиперболата

4.1 Въведение

Една от основните задачи от аналитичната теория на числата е получаването на приближена формула за броя на точките с цели координати (които ще наричаме още цели точки), намиращи се в зададена област в равнината. При определени условия за дадената област, броя на целите точки в нея е приближено равен на лицето ѝ. Задачата се състои в оценка на грешката, която се допуска при това приближение.

Нека, например, нашата област е криволинейния трапец

$$\mathcal{D} = \{ \langle u, v \rangle \in \mathbb{R}^2 \ : \ a < u \leq b \, , \quad 0 < v \leq f(u) \ \},$$

където f е неотрицателна функция, определена в интервала $[a, b]$. Нека $V(\mathcal{D})$ е броя на целите точки $\langle n, m \rangle \in \mathbb{Z}^2$, намиращи се в $\mathcal{D}$. При фиксирано цяло $n \in (a, b]$ броят на целите числа m, за които $0 < m \leq f(n)$ е равен на $[f(n)]$, следователно

$$V(\mathcal{D}) = \sum_{a<n\leq b} [f(n)] \, .$$

Сега използваме формула (2) и получаваме

$$V(\mathcal{D}) = \sum_{a<n\leq b} f(n) - \sum_{a<n\leq b} \{f(n)\}. \tag{172}$$

От горното равенство виждаме, че задачата за намиране на приближена формула за $V(\mathcal{D})$ се разделя на две части: изследване на първата и, съответно, на втората сума от дясната част на (172).

Ако нашата функция f е достатъчно гладка и не осцилира твърде бързо, то изследването на $\sum_{a<n\leq b} f(n)$ не представлява съществена трудност. С помощта на някоя от сумационните формули на Ойлер (виж Леми 2.4 и 2.10) може да се установи, че тази сума не се отличава съществено от интеграла $\int_a^b f(t) \, dt$, който обикновено се пресмята лесно.

Доста по-трудно е изследването на втората сума от дясната част на (172). Ако използваме тривиалното неравенство $0 \leq \{y\} < 1$ виждаме, че тази сума е неотрицателна и не надминава броя на събираемите в нея, т.е. числото $[b] - [a]$. В някои случаи горната оценка е достатъчно добра. Тази оценка обаче е твърде груба, ако се налага по-прецизно изследване на $V(\mathcal{D})$. Тогава се прилага по-сложна техника, базирана на теориите на редовете на Фурие и на експоненциалните суми.

В настоящите записки ще разгледаме две класически задачи от този тип, които са твърде близки една до друга — задачата на Гаус на броя на целите точки в кръга и задачата на Дирихле за броя на целите точки под хиперболата.

4.2 Формулировка на задачата на Гаус за броя на целите точки в кръга. Основни резултати

Задача на Гаус. *Дадено е число $R \geq 2$ и нека $K(R)$ е броят на целите точки в кръг с център началото на координатната система и радиус $\sqrt{R}$, т.е*

$$K(R) = \#\{\ \langle n, m \rangle \in \mathbb{Z}^2\ :\ n^2 + m^2 \leq R\ \}. \tag{173}$$

Да се намери асимптотична формула за $K(R)$ с възможно най-точна оценка за остатъчния член.

От Определение 3.21 виждаме, че $K(R)$ може да се представи още във вида

$$K(R) = \sum_{0 \leq n \leq R} r(n),$$

така че целта е изследването на средната стойност на аритметичната функция $r(n)$.

Като използуваме съображенията от параграф 4.1 можем да предположим, че $K(R)$ е приблизително равно на лицето на кръг с радиус $\sqrt{R}$, т.е. на πR. Да означим с $\Delta_K(R)$ грешката, която допускаме при това приближение, т.е.

$$K(R) = \pi R + \Delta_K(R). \tag{174}$$

Първата оценка на $\Delta_K(R)$ е получена от Гаус чрез използуването само на елементарни средства. Имаме

Теорема 4.1 (Гаус)**.** *При $R \geq 2$ е изпълнено*

$$\Delta_K(R) = O\left(\sqrt{R}\,\right). \tag{175}$$

Доказателство. Нека $\mathcal{G}(R)$ е множеството от целите точки $\langle n, m \rangle$, удовлетворяващи условието в (173). Тогава, разбира се, $K(R) = \#\mathcal{G}(R)$. За всяка точка $\langle n, m \rangle \in \mathcal{G}(R)$ построяваме квадрата $U_{\langle n,m \rangle}$ (включващ и граничните отсечки) с дължина на страната единица, със страни успоредни на координатните оси и с център точката $\langle n, m \rangle$. Да разгледаме обединението на всички тези квадрати:

$$\Gamma(R) = \bigcup_{\langle n,m \rangle \in \mathcal{G}(R)} U_{\langle n,m \rangle}.$$

Ясно е, че $\Gamma(R)$ е многоъгълник с лице равно на $K(R)$.

Нека $\Gamma_1(R)$ и $\Gamma_2(R)$ са кръгове с център началото и радиуси съответно $\sqrt{R} - 1$ и $\sqrt{R} + 1$. Тогава техните лица са равни съответно на

$$K_1(R) = \pi\left(\sqrt{R} - 1\right)^2, \qquad K_2(R) = \pi\left(\sqrt{R} + 1\right)^2.$$

Лесно се вижда, че

$$\Gamma_1(R) \subset \Gamma(R) \subset \Gamma_2(R)$$

(елементарната проверка предоставяме на читателя). Следователно

$$\pi\left(R-2\sqrt{R}+1\right)=K_1(R)\le K(R)\le K_2(R)=\pi\left(R+2\sqrt{R}+1\right).$$

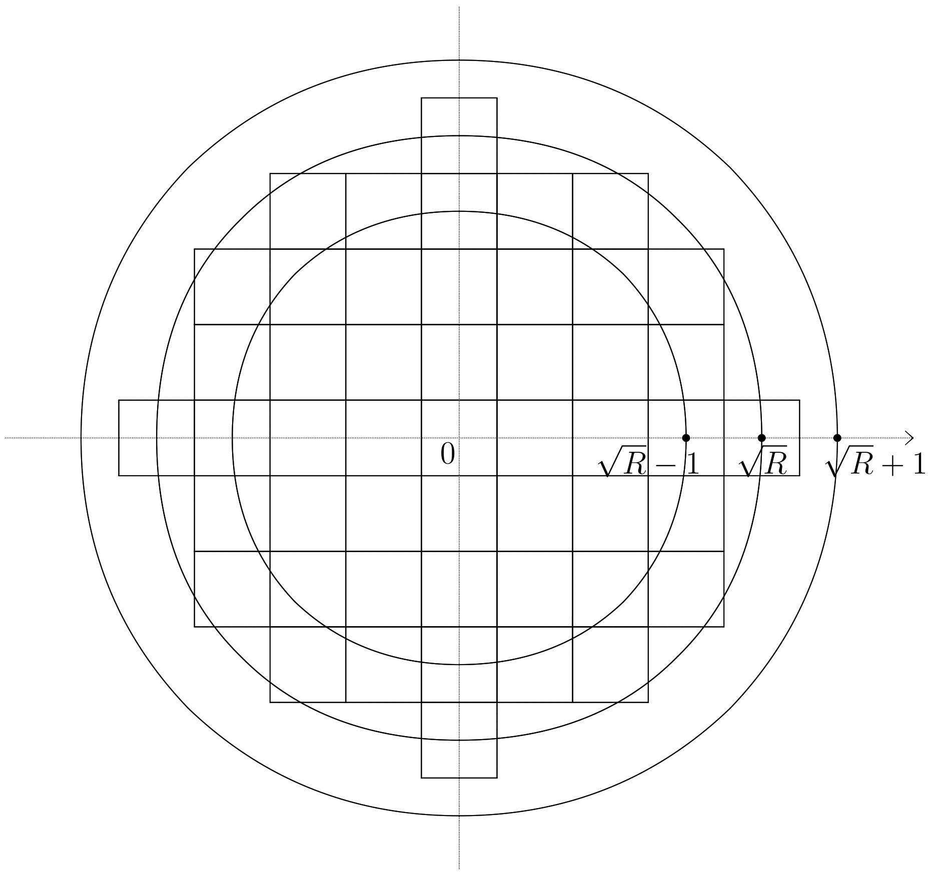
Тогава, ако $\Delta_K(R)$ е определено чрез (174), то имаме

$$|\Delta_K(R)|\le 2\pi\sqrt{R}+\pi, \tag{176}$$

с което теоремата е доказана.

□

Разсъжденията, които проведохме, се илюстрират от следния чертеж.



Първото съществено подобрение на оценката (175) е направено от Вороной през 1903 г. и (независимо) от Серпински през 1906 г. Те доказват следната

Теорема 4.2 (Вороной, Серпински)**.** *Нека* $R\ge 2$*. Тогава е в сила оценката*

$$\Delta_K(R)=O\left(R^{\frac{1}{3}}\,\log R\right). \tag{177}$$

Доказателство на този резултат ще бъде изложено в параграф 4.9 настоящите записки.

Впоследствие степенният показател във дясната част на (177) е подобряван многократно. В настоящия момент най-силният резултат принадлежи на Хаксли. През 2003 г. доказва, че

$$\Delta_K(R) = O_\varepsilon\left(R^{\frac{131}{416}+\varepsilon}\right),$$

където $\varepsilon > 0$ е произволно малко. Да отбележим, че $131/416 = 0.3149\ldots$.

Предполага се, че е вярно следното твърдение:

Хипотеза 4.3 (за броя на целите точки в кръга). *За произволно малко $\varepsilon > 0$ е изпълнено*

$$\Delta_K(R) = O_\varepsilon\left(R^{\frac{1}{4}+\varepsilon}\right). \tag{178}$$

Тази хипотеза все още не е доказана.

От друга страна, още през 1915 г. Харди и Ландау, независимо един от друг, доказват, че оценка от вида (178), но с константа в показателя по-малка от $1/4$ не е възможна. По-точно, тези математици установяват, че за всяко $\varepsilon > 0$ може да се намери редица $\{R_j\}_{j=1}^{\infty}$, такава, че

$$R_j \to \infty, \qquad |\Delta_K(R_j)|\ R_j^{-1/4+\varepsilon} \to \infty \qquad \text{при} \qquad j \to \infty.$$

4.3 Формулировка на задачата на Дирихле за броя на целите точки под хиперболата. Основни резултати

Задача на Дирихле. *Дадено е число $R \geq 2$ и нека $L(R)$ е броят на целите точки от първи квадрант, лежащи под или върху хиперболата $xy = R$, т.е.*

$$L(R) = \#\{\ \langle n, m\rangle \in \mathbb{N}^2\ :\ nm \leq R\ \}. \tag{179}$$

Да се намери асимптотична формула за $L(R)$ с възможно най-точна оценка за остатъчния член.

Да отбележим, че вследствие на Определение 3.17, величината $L(R)$ може да се представи още във вида

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

така че целта на задачата е да се изследва средната стойност на аритметичната функция $\tau(n)$.

С помощта на сравнително прости съображения Дирихле е установил, че при големи стойности на R величината $L(R)$ е приблизително равна на израза

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

където γ е константата на Ойлер. По-точно, ако дефинираме $\Delta_L(R)$ чрез равенството

$$L(R) = R \log R + (2\gamma - 1)R + \Delta_L(R), \tag{180}$$

то имаме

Теорема 4.4 (Дирихле). *При $R \geq 2$ е изпълнено*

$$\Delta_L(R) = O\left(\sqrt{R}\right). \tag{181}$$

Доказателство на тази теорема ще приведем в края на параграф 4.5.

Вороной и (независимо) Серпински подобряват и тази класическа оценка и установяват следната

Теорема 4.5 (Вороной, Серпински). *Нека $R \geq 2$. Тогава е в сила оценката*

$$\Delta_L(R) = O\left(R^{\frac{1}{3}} \log^2 R\right). \tag{182}$$

Доказателството на тази теорема ще бъде дадено в параграф 4.10 от настоящите записки.

Степенният показател в дясната част на (182) е подобряван много пъти и рекордът принадлежи отново на Хаксли. През 2003 г. той доказва, че този показател може да бъде взет $\frac{131}{416} + \varepsilon$, където $\varepsilon > 0$ е произволно малко.

И по отношение на задачата на Дирихле е изказана хипотеза, която все още не е доказана:

Хипотеза 4.6 (за броя на целите точки под хиперболата). *За произволно малко $\varepsilon > 0$ е изпълнено*

$$\Delta_L(R) = O_\varepsilon\left(R^{\frac{1}{4}+\varepsilon}\right). \tag{183}$$

През 1916 г. Харди е установил, че показателят $\frac{1}{4}$ в (183) не може да бъде заменен с по-малко число.

4.4 Формула за остатъчния член в задачата на Гаус

Като използваме втората сумационна формула на Ойлер (Лема 2.10), ще запишем остатъчния член $\Delta_K(R)$ в задачата на Гаус във вид удобен за по-нататъшно изследване.

Лема 4.7. *Величината $\Delta_K(R)$, определена чрез* (174)*, може да се запише във вида*

$$\Delta_K(R) = 8\,\Delta_K^*(R) + O(1), \tag{184}$$

където

$$\Delta_K^*(R) = \sum_{n \leq \sqrt{R/2}} \rho\left(\sqrt{R - n^2}\right) \tag{185}$$

и $\rho(t)$ е функцията от Определение 2.2.

Забележка. От (185) и от Лема 2.3 (2) тривиално следва, че $|\Delta_0^*(R)| \le \frac{1}{2}\sqrt{R/2}$. Тогава, като вземем предвид (184) получаваме отново оценката $\Delta_K(R) = O(\sqrt{R})$, която вече ни е известна от Теорема 4.1. Но, както ще видим в следващите параграфи, формулите от Лема 4.7 ни дават възможност да оценим $\Delta_K(R)$ много по-точно и по този начин да докажем Теорема 4.2.

Доказателство. Ясно е, че броят на целите точки в кръг с център началото и радиус $\sqrt{R}$, лежащи на някоя от координатните оси, е равен на $4\left[\sqrt{R}\right] + 1$. Да означим

$$K_1(R) = \#\left\{\langle n, m\rangle \in \mathbb{N}^2 \;:\; n^2 + m^2 \le R\right\}$$

и тогава имаме

$$K(R) = 4K_1(R) + 4\left[\sqrt{R}\right] + 1. \tag{186}$$

Да разгледаме $K_1(R)$. Като използуваме съображенията, изложени в параграф 4.1, получаваме

$$K_1(R) = \sum_{n \le \sqrt{R}} \left[\sqrt{R - n^2}\right].$$

Тази формула обаче не е подходяща за изследване на $K_1(R)$. Причината е в това, че когато x е близо до $\sqrt{R}$, модулът на втората производна на функцията $\sqrt{R - x^2}$ е твърде голям и това възпрепятства успешното прилагане на Лема 2.10.

Значително по-удобно се работи по следния начин. Нека

$$\begin{aligned}
K_2(R) &= \#\left\{\langle n, m\rangle \in \mathbb{N}^2 \;:\; n^2 + m^2 \le R, \quad n \le \sqrt{R/2}\right\},\\
K_3(R) &= \#\left\{\langle n, m\rangle \in \mathbb{N}^2 \;:\; n^2 + m^2 \le R, \quad m \le \sqrt{R/2}\right\}.
\end{aligned}$$

Поради симетрията имаме $K_2(R) = K_3(R)$. Също така, точките $\langle n, m\rangle \in \mathbb{N}^2$, за които $n, m \le \sqrt{R/2}$ са преброени както в $K_2(R)$, така и в $K_3(R)$. Следователно

$$K_1(R) = 2K_2(R) - \left[\sqrt{R/2}\,\right]^2. \tag{187}$$

От (2), (186) и (187) следва

$$\begin{aligned}
K(R) &= 8K_2(R) - 4\left[\sqrt{R/2}\,\right]^2 + 4\left[\sqrt{R}\right] + 1\\
&= 8K_2(R) - 4\left(\sqrt{R/2} - \left\{\sqrt{R/2}\right\}\right)^2 + 4\left(\sqrt{R} - \left\{\sqrt{R}\right\}\right) + 1\\
&= 8K_2(R) - 2R + 4\sqrt{2R}\left\{\sqrt{R/2}\right\} + 4\sqrt{R} + O(1).
\end{aligned} \tag{188}$$

Да разгледаме $K_2(R)$. Отново разсъждаваме, както в параграф 4.1. За всяко фиксирано $n \in \mathbb{N}$, за което $n \le \sqrt{R/2}$ броят на числата $m \in \mathbb{N}$, удовлетворяващи $n^2 + m^2 \le R$ е равен на $\left[\sqrt{R - m^2}\right]$. Следователно

$$K_2(R) = \sum_{n \le \sqrt{R/2}} \left[\sqrt{R - n^2}\right].$$

Сега, като се възползуваме от (2), получаваме

$$K_2(R) = K^*(R) - K'(R), \tag{189}$$

където

$$K^*(R) = \sum_{n\le\sqrt{R/2}} \sqrt{R-n^2}, \qquad K'(R) = \sum_{n\le\sqrt{R/2}} \left\{\sqrt{R-n^2}\right\}. \tag{190}$$

Да разгледаме величината $K^*(R)$. Прилагаме Лема 2.10 при $a = 0$, $b = \sqrt{R/2}$, $f(x) = \sqrt{R-x^2}$ и получаваме

$$K^*(R) = \int\limits_0^{\sqrt{R/2}} \sqrt{R-t^2}\,dt + \rho\left(\sqrt{R/2}\right) f\left(\sqrt{R/2}\right) - \rho(0)f(0)$$

$$- \sigma\left(\sqrt{R/2}\right) f'\left(\sqrt{R/2}\right) + \sigma(0)\, f'(0) + \int\limits_0^{\sqrt{R/2}} \sigma(t) f''(t)\,dt. \tag{191}$$

Имаме

$$f'(x) = -x\left(R-x^2\right)^{-\frac{1}{2}}, \qquad f''(x) = -R\left(R-x^2\right)^{-\frac{3}{2}}. \tag{192}$$

От последната формула следва, че $|f''(t)| \le 2^{\frac{3}{2}}\, R^{-\frac{1}{2}}$ при $0 \le t \le \sqrt{R/2}$. Като вземем предвид също Лема 2.9 (2), получаваме

$$\left|\int\limits_0^{\sqrt{R/2}} \sigma(t) f''(t)\,dt\right| \le \int\limits_0^{\sqrt{R/2}} |\sigma(t) f''(t)|\,dt \le \int\limits_0^{\sqrt{R/2}} \frac{1}{8}\, 2^{\frac{3}{2}}\, R^{-\frac{1}{2}} = \frac{1}{4}. \tag{193}$$

По-нататък, лесно се установява, че

$$\int\limits_0^{\sqrt{R/2}} \sqrt{R-t^2}\,dt = \frac{\pi R}{8} + \frac{R}{4} \tag{194}$$

(проверката предоставяме на читателя). От (191) – (194) следва

$$K^*(R) = \frac{\pi R}{8} + \frac{R}{4} + \rho\left(\sqrt{R/2}\right)\sqrt{R/2} - \frac{1}{2}\sqrt{R} + O(1). \tag{195}$$

От (7), (188), (189) и (195) след прости пресмятания получаваме

$$K(R) = \pi R + 4\sqrt{R/2} - 8\sum_{n\le\sqrt{R/2}} \left\{\sqrt{R-n^2}\right\} + O(1).$$

Оттук и от (7) намираме, че

$$K(R) = \pi R + 8\Delta_K^*(R) + O(1), \tag{196}$$

където $\Delta_K^*(R)$ е определено чрез (185). Тогава, като вземем предвид (174), получаваме доказателството на лемата.

$\square$

4.5 Формула за остатъчния член в задачата на Дирихле

В следващата лема ще установим, че и остатъчния член $\Delta_L(R)$ в задачата на Дирихле може да бъде записан във вид удобен за по-нататъшно иследване.

Лема 4.8. *Величината* $\Delta_L(R)$*, определена чрез* (180)*, може да се запише във вида*

$$\Delta_L(R) = 2\Delta_L^*(R) + O(1) \tag{197}$$

където

$$\Delta_L^*(R) = \sum_{n\le\sqrt{R}} \rho\left(\frac{R}{n}\right) \tag{198}$$

и $\rho(t)$ *е функцията от Определение 2.2.*

Доказателство. Да означим

$$\begin{aligned} L_1(R) &= \#\left\{\langle n,m\rangle \in \mathbb{N}^2 \ :\ nm \le R, \quad n \le \sqrt{R}\right\}, \\ L_2(R) &= \#\left\{\langle n,m\rangle \in \mathbb{N}^2 \ :\ nm \le R, \quad m \le \sqrt{R}\right\}. \end{aligned}$$

Поради симетрията имаме $L_1(R) = L_2(R)$. Също така, точките $\langle n,m\rangle \in \mathbb{N}^2$, за които $n, m \le \sqrt{R}$ са преброени както в $L_1(R)$, така и в $L_2(R)$. Следователно

$$L(R) = 2L_1(R) - \left[\sqrt{R}\,\right]^2. \tag{199}$$

За да изследваме $L_1(R)$ прилагаме отново съображенията от параграф 4.1. За всяко фиксирано $n \in \mathbb{N}$, за което $n \le \sqrt{R}$, броят на числата $m \in \mathbb{N}$, удовлетворяващи $nm \le R$, е равен на $[R/n]$. Следователно

$$L_1(R) = \sum_{n\le\sqrt{R}} \left[\frac{R}{n}\right] = \sum_{n\le\sqrt{R}} \left(\frac{R}{n} - \left\{\frac{R}{n}\right\}\right) = R\sum_{n\le\sqrt{R}} \frac{1}{n} - L'(R),$$

където

$$L'(R) = \sum_{n\le\sqrt{R}} \left\{\frac{R}{n}\right\}. \tag{200}$$

Сега, като приложим Лема 2.11 и използуваме определението (7) за $\rho(t)$, намираме

$$\begin{aligned} L_1(R) &= R\left(\log\sqrt{R} + \gamma + \frac{\rho\left(\sqrt{R}\right)}{\sqrt{R}} + O\left(\frac{1}{R}\right)\right) - L'(R) \\ &= \frac{1}{2}R\log R + \gamma R + \frac{1}{2}\sqrt{R} - \sqrt{R}\left\{\sqrt{R}\right\} - L'(R) + O(1). \end{aligned}$$

Оттук и от (199) получаваме

$$\begin{aligned} L(R) &= R\log R + 2\gamma R + \sqrt{R} - 2\sqrt{R}\left\{\sqrt{R}\right\} - 2L'(R) - \left(\sqrt{R} - \left\{\sqrt{R}\right\}\right)^2 + O(1) \\ &= R\log R + (2\gamma - 1)R + \sqrt{R} - 2L'(R) + O(1). \end{aligned}$$

Тогава, като вземем предвид (7) и (200), получаваме

$$L(R) = R \log R + (2\gamma - 1)R + 2 \sum_{n \le \sqrt{R}} \rho\left(\frac{R}{n}\right) + O(1).$$

От последната формула и от определението (180) за $\Delta_L(R)$ следва (197), с което лемата е доказана.

□

Както ще видим по-нататък, резултатът на Лема 4.8 ще послужи като отправна точка, от която ще тръгнем, за да докажем Теорема 4.5. Засега ще дадем доказателството на теоремата на Дирихле.

Доказателство на Теорема 4.4. От (197), (198) и Лема 2.3 (2) получаваме оценката $\Delta_L(R) = O\left(\sqrt{R}\right)$, с което твърдението е доказано.

□

4.6 Редът на Фурие на функцията $\rho(t)$.

Както вече знаем, функцията $\rho(t)$ е периодична с период 1 и поради това ѝ съответства ред на Фурие. В настоящия параграф ще изследваме частичните суми на този ред и връзката им с $\rho(t)$.

Първо ще споменем някои елементарни, но важни факти, отнасящи се за функцията $e(t)$, определена чрез (3).

Лема 4.9. *Функцията $e(t)$ притежава свойствата:*

(1) *$e(t)$ е периодична с период 1.*

(2) *При $t \in \mathbb{R}$ е изпълнено $|e(t)| = 1$.*

(3) *При $n \in \mathbb{Z}$ е изпълнено $e(n) = 1$.*

(4) *За произволни $t, t' \in \mathbb{C}$ имаме $e(t + t') = e(t)e(t')$.*

(5) *Ако $n \in \mathbb{Z}$, то*

$$\int_0^1 e(tn)\, dt = \begin{cases} 1 & \text{при} \quad n = 0, \\ 0 & \text{при} \quad n \ne 0. \end{cases}$$

(6) *Ако $n \in \mathbb{Z}$, $q \in \mathbb{N}$, то*

$$\sum_{k=1}^{q} e\left(\frac{kn}{q}\right) = \begin{cases} q & \text{при} \quad n \equiv 0 \pmod q, \\ 0 & \text{в противен случай.} \end{cases}$$

Доказателство. Проверката на (1) – (5) следва директно от свойствата на експоненциалната функция, а за проверката на (6) използуваме формулата за сума от членовете на геометрична прогресия.

$\square$

За да продължим по-нататък, ще ни е нужна следната

Лема 4.10. *Нека $M \in \mathbb{Z}, H \in \mathbb{N}$ и $t \in \mathbb{R}$. Тогава за сумата*

$$K(t) = \sum_{k=M+1}^{M+H} e(tk) \tag{201}$$

е в сила неравенството

$$|K(t)| \leq \min\left(H, \frac{1}{2||t||}\right). \tag{202}$$

Забележка. При $t \in \mathbb{Z}$ имаме $||t|| = 0$ и изразът в дясната част на (202) е неопределен. За да избегнем това неудобство, ще считаме, че $\min\left(H, \frac{1}{0}\right) = H$.

Доказателство. От неравенството на триъгълника и от Лема 4.9 (2) веднага получаваме неравенството $|K(t)| \leq H$. Остава да докажем, че

$$|K(t)| \leq \frac{1}{2||t||} \qquad \text{при} \qquad t \notin \mathbb{Z}.$$

От (201), Лема 4.9 и от определението на $||t||$ се вижда, че функциите $|K(t)|$ и $||t||^{-1}$ са четни, а също периодични с период 1. Следователно, достатъчно е да докажем, че

$$|K(t)| \leq \frac{1}{2t} \qquad \text{при} \qquad 0 < t \leq \frac{1}{2}. \tag{203}$$

Като се възползваме от (3), Лема 4.9 (2), формулата на Ойлер

$$\sin u = \frac{e^{iu} - e^{-iu}}{2i} \tag{204}$$

и от формулата за сумата от членовете на геометрична прогресия, намираме

$$|K(t)| = \left|e(t(M+1))\frac{1-e(tH)}{1-e(t)}\right| = \left|\frac{1-e(tH)}{1-e(t)}\right| \leq \frac{2}{\left|e\left(-\frac{t}{2}\right) - e\left(\frac{t}{2}\right)\right|} = \frac{1}{\sin(\pi t)}.$$

Остава да забележим, че функцията $\sin(\pi t)$ е вдлъбната при $0 \leq t \leq \frac{1}{2}$ откъдето следва, че за тези стойности на t е изпълнено $\sin(\pi t) \geq 2t$. Оттук получаваме (203), с което лемата е доказана.

$\square$

Следващата лема ни дава възможност да приближаваме функцията $\rho(t)$ с крайна сума, като грешката се оценява в зависимост от дължината на тази сума.

Лема 4.11. *Нека $M \in \mathbb{R}$, $M \geq 2$. Тогава за всяко $t \in \mathbb{R}$ е в сила неравенството*

$$\left|\rho(t) - \sum_{1 \leq |n| \leq M} \frac{e(nt)}{2\pi i n}\right| \leq \min\left(1, \frac{1}{M||t||}\right). \tag{205}$$

Доказателство. Тъй като функциите от двете страни на (205) са периодични с период 1, достатъчно е да докажем това неравенство при $0 \le |t| \le \frac{1}{2}$. При $t = 0$ то е очевидно, следователно можем да считаме, че

$$0 < |t| \le \frac{1}{2}. \tag{206}$$

Редът на Фурие, отговарящ на функцията $\rho(t)$, е $\sum_{n=1}^{\infty} \frac{1}{\pi n} \sin(2\pi n t)$. От теорията на редовете на Фурие и от Лема 2.3 (3), (4) следва, че

$$\sum_{n=1}^{\infty} \frac{\sin(2\pi n t)}{\pi n} = \begin{cases} \rho(t) & \text{ако} \quad t \notin \mathbb{Z}, \\ 0 & \text{ако} \quad t \in \mathbb{Z}. \end{cases} \tag{207}$$

Като приложим (204) виждаме, че сумата, намираща се в лявата страна на неравенството (205) може да бъде записана в друг вид, а именно

$$\sum_{1 \le |n| \le M} \frac{e(nt)}{2\pi i n} = \sum_{1 \le n \le M} \frac{\sin(2\pi n t)}{\pi n}. \tag{208}$$

При произволно $N > M$ прилагаме преобразованието на Абел (Лема 2.1) при

$$\lambda_n = n, \qquad f(x) = \frac{1}{x}, \qquad g_n = \sin(2\pi n t)$$

и получаваме

$$\begin{aligned} \left| \sum_{M < n \le N} \frac{\sin(2\pi n t)}{\pi n} \right| &= \left| -\frac{1}{\pi} \int_M^N \left(\sum_{M < n \le u} \sin(2\pi n t) \right) \frac{-1}{u^2}\, du + \frac{1}{\pi N} \sum_{M < n \le N} \sin(2\pi n t) \right| \\ &\le \frac{1}{\pi} \int_M^N \left| \sum_{M < n \le u} \sin(2\pi n t) \right| \frac{du}{u^2} + \frac{1}{\pi N} \left| \sum_{M < n \le N} \sin(2\pi n t) \right|. \end{aligned} \tag{209}$$

Но от Лема 4.10, формули (3), (204) и от нашето допускане (206) следва

$$\begin{aligned} \left| \sum_{M < n \le u} \sin(2\pi n t) \right| &= \left| \sum_{M < n \le u} \frac{e(nt) - e(-nt)}{2i} \right| \\ &\le \frac{1}{2} \left| \sum_{M < n \le u} e(nt) \right| + \frac{1}{2} \left| \sum_{M < n \le u} e(-nt) \right| \le \frac{1}{2||t||} = \frac{1}{2|t|}. \end{aligned}$$

Като заместим последната оценка в (209) виждаме, че

$$\left| \sum_{M < n \le N} \frac{\sin(2\pi n t)}{\pi n} \right| \le \frac{1}{2\pi |t|} \left(\int_M^N \frac{du}{u^2} + \frac{1}{N} \right) = \frac{1}{2\pi |t| M}.$$

Извършваме в последното неравенство граничен преход $N \to \infty$ и получаваме

$$\left| \sum_{M<n} \frac{\sin(2\pi n t)}{\pi n} \right| \le \frac{1}{2\pi |t| M}. \tag{210}$$

От (206) – (208) и (210) следва

$$\left| \rho(t) - \sum_{1 \le n \le M} \frac{\sin(2\pi n t)}{\pi n} \right| \le \frac{1}{2\pi |t| M}.$$

От последното неравенство се получава (205) в случая $\frac{1}{2\pi M} \le |t| \le \frac{1}{2}$. Наистина, тогава имаме

$$\frac{1}{2\pi M |t|} = \min\left(1, \frac{1}{2\pi M |t|}\right) \le \min\left(1, \frac{1}{M|t|}\right) = \min\left(1, \frac{1}{M||t||}\right)$$

и, като вземем предвид (208), заключаваме, че в разглеждания случай (205) е вярно.

Нека сега е изпълнено $0 < |t| \le \frac{1}{2\pi M}$. Тогава, като използуваме (208), Лема 2.3 (2) и известното неравенство $|\sin u| \le |u|$, получаваме

$$\begin{aligned}\left| \rho(t) - \sum_{1 \le n \le M} \frac{\sin(2\pi n t)}{\pi n} \right| &\le |\rho(t)| + \sum_{1 \le n \le M} \frac{|\sin(2\pi n t)|}{\pi n} \le \frac{1}{2} + \sum_{1 \le n \le M} \frac{2\pi n |t|}{\pi n} \le \frac{1}{2} + 2|t|M \\ &\le \frac{1}{2} + \frac{1}{\pi} \le 1 = \min\left(1, \frac{1}{2\pi M |t|}\right) = \min\left(1, \frac{1}{2\pi M ||t||}\right).\end{aligned}$$

Оттук следва, че (205) е вярно и в този случай. С това лемата е доказана.

$\square$

В следващата лема се дава информация за коефициентите на Фурие на функцията от дясната част на неравенството (205).

Лема 4.12. *Нека $M \in \mathbb{R}$, $M \ge 2$ Тогава за всяко $t \in \mathbb{R}$ е изпълнено*

$$\min\left(1, \frac{1}{M||t||}\right) = \sum_{n \in \mathbb{Z}} b_M(n)\, e(nt), \tag{211}$$

като

$$|b_M(n)| \le \begin{cases} \frac{4 \log M}{M} & \text{при} \quad n \in \mathbb{Z}, \\ \frac{M}{n^2} & \text{при} \quad n \in \mathbb{Z},\ n \ne 0. \end{cases} \tag{212}$$

Доказателство. От теорията на редовете на Фурие знаем, че ако определим

$$b_M(n) = \int_{-\frac{1}{2}}^{\frac{1}{2}} \min\left(1, \frac{1}{M||t||}\right) e(-nt)\, dt, \tag{213}$$

то (211) е изпълнено за всяко $t \in \mathbb{R}$. Представяме последния интеграл като сума от два интеграла $I_1 + I_2$, където в I_1 интегрираме по интервала $[-\frac{1}{2}, 0]$, а в I_2 — по интервала $[0, \frac{1}{2}]$. След смяна на променливата получаваме

$$I_1 = \int\limits_0^{\frac{1}{2}} \min\left(1, \frac{1}{Mt}\right) e(nt)\, dt.$$

Тогава, като вземем предвид формулата на Ойлер

$$\cos u = \frac{e^{iu} + e^{-iu}}{2}$$

виждаме, че

$$b_M(n) = \int\limits_0^{\frac{1}{2}} \min\left(1, \frac{1}{Mt}\right) \big(e(nt) + e(-nt)\big)\, dt = 2\int\limits_0^{\frac{1}{2}} \min\left(1, \frac{1}{Mt}\right) \cos(2\pi nt)\, dt. \quad (214)$$

Тогава за всяко $n \in \mathbb{Z}$ имаме

$$|b_M(n)| \leq 2\int\limits_0^{\frac{1}{2}} \min\left(1, \frac{1}{Mt}\right) dt = 2\int\limits_0^{\frac{1}{M}} dt + \frac{2}{M}\int\limits_{\frac{1}{M}}^{\frac{1}{2}} \frac{dt}{t} = \frac{2}{M}\left(1 - \log 2 + \log M\right) \leq \frac{4\log M}{M}.$$

Нека сега $n \neq 0$. От (214) следва

$$b_M(n) = 2\int\limits_0^{\frac{1}{M}} \cos(2\pi nt)\, dt + \frac{2}{M}\int\limits_{\frac{1}{M}}^{\frac{1}{2}} \frac{\cos(2\pi nt)}{t}\, dt.$$

Първият от горните два интеграла е табличен и се пресмята непосредствено. Втория интеграл преобразуваме, като вкараме косинуса под знака на диференциала, след което интегрираме по части. Получаваме

$$\begin{aligned}
b_M(n) &= \frac{1}{\pi n}\left(\sin\frac{2\pi n}{M} + \frac{1}{M}\int\limits_{\frac{1}{M}}^{\frac{1}{2}} \frac{d\sin(2\pi nt)}{t}\right) \\
&= \frac{1}{\pi n}\left(\sin\frac{2\pi n}{M} + \frac{1}{M}\left(\frac{\sin \pi n}{\frac{1}{2}} - \frac{\sin\frac{2\pi n}{M}}{\frac{1}{M}} + \int\limits_{\frac{1}{M}}^{\frac{1}{2}} \frac{\sin(2\pi nt)}{t^2}\, dt\right)\right) \\
&= \frac{1}{\pi n M}\int\limits_{\frac{1}{M}}^{\frac{1}{2}} \frac{\sin(2\pi nt)}{t^2}\, dt
\end{aligned}$$

Сега, като вкараме синуса под знака на диференциала и интегрираме по части, намираме, че

$$b_M(n) = \frac{-1}{2\pi^2 n^2 M} \int\limits_{\frac{1}{M}}^{\frac{1}{2}} \frac{d\cos(2\pi nt)}{t^2} = \frac{-1}{2\pi^2 n^2 M} \left(\frac{\cos \pi n}{\left(\frac{1}{2}\right)^2} - \frac{\cos \frac{2\pi n}{M}}{\left(\frac{1}{M}\right)^2} + 2 \int\limits_{\frac{1}{M}}^{\frac{1}{2}} \frac{\cos(2\pi nt)}{t^3}\, dt \right).$$

Оттук и от неравенството на триъгълника следва, че при $n \neq 0$ имаме

$$|b_M(n)| \leq \frac{1}{2\pi^2 n^2 M} \left(4 + M^2 + 2 \int\limits_{\frac{1}{M}}^{\infty} \frac{dt}{t^3} \right) = \frac{4 + 2M^2}{2\pi^2 n^2 M} \leq \frac{M}{n^2}.$$

С това лемата е доказана.

□

4.7 Теорема за оценка на експоненциална сума

При изследването на много задачи от теорията на числата се появява експоненциалната сума

$$S = \sum_{a<n\leq b} e(f(n)),$$

където $f(x)$ е реалнозначна функция, определена в $[a, b]$. В някои (редки) случаи сумата S може да се изрази чрез явна формула, но в общия случай това не е възможно. Въпреки това задачите, при изследването на които възниква S, често получават задоволително решение само ако използуваме нетривиална оценка за модула на сумата S. За да поясним, ще споменем, че очевидното неравенство

$$|S| \leq \sum_{a<n\leq b} 1 = [b] - [a]$$

се нарича тривиална оценка за S, а всяка оценка, която е по-силна от тривиалната, се нарича нетривиална.

Разбира се, не винаги нашата сума може да се оцени нетривиално. Например, ако $f(n) \in \mathbb{Z}$ за всяко цяло $n \in (a, b]$, то $S = \sum_{a<n\leq b} 1 = [b] - [a]$. Да допуснем обаче, че дробните части на $f(n)$ са равномерно разпределени, когато n пробгва целите числа от $(a, b]$ (тук няма да даваме строго определение на това понятие). Тогава комплексните числа $e(f(n))$, разглеждани като единични вектори в равнината, при сумирането им „се унищожават” взаимно и поради това можем да очакваме, че $|S|$ е много по-малко от $[b] - [a]$, т.е. ще има нетривиална оценка за нашата сума.

Изказаната идея може да се реализира на практика, стига да разполагаме с подходяща аналитична информация за функцията $f(x)$. В настоящия параграф ще докажем един важен резултат от такъв тип — Теорема 4.16, известна като *оценка на Ван-дер-Корпут*. Грубо казано, тя гласи, че ако втората производна $f''(x)$ е по модул „малка”, но не „прекалено малка”, то сумата S може да се оцени нетривиално.

За доказателството на Теорема 4.16 са ни нужни две помощни леми. Първата от тях гласи, че при определени условия за функцията $f(x)$ нашата сума S с голяма точност се приближава със сума от експоненциални интеграли. Читателите, запознати с формулата на Поасон, ще забележат връзката между нея и равенството в следващата лема. Имаме

Лема 4.13. *Нека числата a и b са от вида $k+\frac{1}{2}$, $k \in \mathbb{Z}$, като $b-a>2$. Нека функцията $f(x)$ е два пъти непрекъснато диференцируема в интервала $[a,b]$ и нека $f''(x)>0$ при $x \in [a,b]$. Тогава е в сила формулата*

$$\sum_{a<n\le b} e(f(n)) = \sum_{f'(a)-1\le n\le f'(b)+1} \int\limits_a^b e(f(x)-nx)\,dx + O\big(\log\left(f'(b)-f'(a)+2\right)\big), \quad (215)$$

като константата в знака O е абсолютна.

Забележка. Може да се докаже, че горната формула е вярна за произволни реални a,b удовлетворяващи $b-a>0$. Също така, сумирането в дясната страна на (215) може да се вземе по $n \in [f'(a)-\theta, f'(b)+\theta]$ за произволно $\theta \in (0,1]$, но тогава трябва да се добави допълнителен остатъчен член $O\left(\theta^{-1}\right)$. За нашите цели обаче лемата в настоящия ѝ вид е достатъчно удобна.

Доказателство. Нека за простота положим

$$A = f'(a), \qquad B = f'(b) \quad (216)$$

и нека означим с S сумата от лявата страна на (215). Прилагаме Лема 2.4 и получаваме

$$S = \int\limits_a^b e\left(f(x)\right)\,dx + \rho(b)e(f(b)) - \rho(a)e(f(a)) - \int\limits_a^b \rho(x)\,\left(\frac{d}{dx}e(f(x))\right)\,dx$$

$$= \int\limits_a^b e\left(f(x)\right)\,dx + O(1) - \int\limits_a^b \rho(x)\,\left(\frac{d}{dx}e(f(x))\right)\,dx. \quad (217)$$

Взимаме произволно $M \ge |A|+|B|+2$ и, като приложим Лема 4.11, виждаме, че за всяко x е изпълнено

$$\rho(x) = \sum_{1\le|n|\le M} \frac{e(nx)}{2\pi i n} + O\left(\min\left(1, \frac{1}{M||x||}\right)\right).$$

Заместваме в (217) и намираме

$$S = \int\limits_a^b e\left(f(x)\right)\,dx + O(1)$$

$$- \int\limits_a^b \left(\sum_{1\le|n|\le M} \frac{e(nx)}{2\pi i n} + O\left(\min\left(1, \frac{1}{M||x||}\right)\right)\right)\left(\frac{d}{dx}\, e(f(x))\right)\,dx$$

$$= \int\limits_a^b e\left(f(x)\right)\,dx + O(1) - \Sigma_1 + O(\Sigma_2), \tag{218}$$

където

$$\Sigma_1 = \sum_{1\le|n|\le M} \frac{1}{2\pi i n}\, I_n\,, \qquad I_n = \int\limits_a^b e(nx)\left(\frac{d}{dx}\, e(f(x))\right)\,dx, \tag{219}$$

$$\Sigma_2 = \int\limits_a^b \min\left(1, \frac{1}{M||x||}\right)\,|f'(x)|\,dx.$$

Да разгледаме сумата Σ_2. Знаем, че функцията $\min\left(1, (M||x||)^{-1}\right)$ е периодична с период 1 и, също така, непосредствено се проверява, че

$$\int\limits_0^1 \min\left(1, \frac{1}{M||x||}\right)\,dx \ll \frac{\log M}{M}.$$

Тогава

$$\Sigma_2 \le \max_{a\le x\le b} |f'(x)| \int\limits_a^b \min\left(1, \frac{1}{M||x||}\right)\,dx \ll (b-a)\,\frac{\log M}{M} \max_{a\le x\le b} |f'(x)|. \tag{220}$$

Сега да разгледаме сумата Σ_1, определена чрез (219). За тази цел интегрираме по части интеграла I_n и, като използваме, че a и b са от вида, $k+\frac{1}{2}$, $k\in\mathbb{Z}$, получаваме

$$I_n = \Big(e(f(b)) - e(f(a))\Big)(-1)^n - 2\pi i\, n \int\limits_a^b e(f(x)+nx)\,dx.$$

Тогава, като съобразим, че $\sum_{1\le|n|\le M} \frac{(-1)^n}{n} = 0$ намираме

$$\Sigma_1 = -\sum_{1\le|n|\le M} \int\limits_a^b e\left(f(x)+nx\right)\,dx = -\sum_{1\le|n|\le M} J_n, \tag{221}$$

където

$$J_n = \int_a^b e\left(f(x) - nx\right)\, dx. \tag{222}$$

От (218), (220) и (221) следва

$$S = \Sigma_3 + O(1) + O\left((b-a)\, \frac{\log M}{M} \max_{a \le x \le b} |f'(x)| \right), \tag{223}$$

където константите в знаците O са абсолютни и

$$\Sigma_3 = \sum_{|n| \le M} J_n. \tag{224}$$

Представяме Σ_3 във вида

$$\Sigma_3 = \Sigma_4 + \Sigma_5 + \Sigma_6, \tag{225}$$

където

$$\Sigma_4 = \sum_{A-1 \le n \le B+1} J_n, \qquad \Sigma_5 = \sum_{-M \le n < A-1} J_n, \qquad \Sigma_6 = \sum_{B+1 < n \le M} J_n. \tag{226}$$

Да разгледаме сумата Σ_6. За тази цел ще изследваме интеграла J_n, определен чрез (222). По условие $f''(x) > 0$, следователно функцията $f'(x)$ е растяща и, тъй като $n > B+1 = f'(b)+1$, имаме $f'(x) \ne n$ при $x \in [a, b]$. Тогава, като интегрираме по части и използваме (216) и допускането, че a и b са от вида $k + \frac{1}{2}$, $k \in \mathbb{Z}$, получаваме

$$\begin{aligned}
J_n &= \int_a^b e\left(f(x) - nx\right)\, \frac{f'(x) - n}{f'(x) - n}\, dx = \int_a^b e\left(f(x) - nx\right)\, \frac{d\left(f(x) - nx\right)}{f'(x) - n} \\
&= \frac{1}{2\pi i} \int_a^b \frac{d\, e\left(f(x) - nx\right)}{f'(x) - n} \\
&= \frac{1}{2\pi i} \left(\frac{e\left(f(b) - nb\right)}{f'(b) - n} - \frac{e\left(f(a) - na\right)}{f'(a) - n} + F_n \right) \\
&= \frac{1}{2\pi i} \left(e(f(b)) \frac{(-1)^n}{B - n} - e(f(a)) \frac{(-1)^n}{A - n} + F_n \right),
\end{aligned} \tag{227}$$

където

$$F_n = \int_a^b e\left(f(x) - nx\right)\, \frac{f''(x)}{\left(f'(x) - n\right)^2}\, dx. \tag{228}$$

От (226) и (227) получаваме

$$|\Sigma_6| \leq \left| \sum_{B+1<n\leq M} \frac{(-1)^n}{n-B} \right| + \left| \sum_{B+1<n\leq M} \frac{(-1)^n}{n-A} \right| + \sum_{B+1<n\leq M} |F_n|. \tag{229}$$

Ясно е, че за произволно M е изпълнено

$$\left| \sum_{B+1<n\leq M} \frac{(-1)^n}{n-A} \right| \leq 1, \qquad \left| \sum_{B+1<n\leq M} \frac{(-1)^n}{n-B} \right| \leq 1. \tag{230}$$

Сега ще оценим и последната сума в дясната страна на (229). От (216) и (228) намираме

$$|F_n| \leq \int\limits_a^b \frac{f''(x)}{\left(f'(x)-n\right)^2}\, dx = \int\limits_a^b \frac{d\left(f'(x)-n\right)}{\left(f'(x)-n\right)^2} = \frac{1}{n-B} - \frac{1}{n-A}. \tag{231}$$

От Лема 2.5 следва

$$\sum_{B+1<n\leq M} \frac{1}{n-B} = \int\limits_{B+1}^{M} \frac{dt}{t-B} + O\left(1\right) = \log(M-B) + O\left(1\right) \tag{232}$$

и аналогично

$$\sum_{B+1<n\leq M} \frac{1}{n-A} = \log(M-A) - \log(B-A+1) + O\left(1\right). \tag{233}$$

Тогава от (231) – (233) получаваме

$$\sum_{B+1<n\leq M} |F_n| \ll \log(B-A+2). \tag{234}$$

От (229), (230) и (234) следва

$$\Sigma_6 \ll \log(B-A+2).$$

По аналогичен начин получаваме също

$$\Sigma_5 \ll \log(B-A+2).$$

От последните две формули и от (225) получаваме

$$\Sigma_3 = \Sigma_4 + O\big(\log(B-A+2)\big), \tag{235}$$

като константата в знака O е абсолютна. Заместваме последния израз вместо Σ_3 в (223) и виждаме, че като изберем достатъчно голямо M се получава (215).

$\square$

В следващите две леми ще приведем оценки за експоненциални интеграли от вида

$$I = \int_a^b e(f(x))\,dx. \tag{236}$$

В първата от тях ще видим, че модулът на интеграла е „малък”, ако производната $f'(x)$ е монотонна и „голяма”. По-точно, имаме

Лема 4.14. *Нека функцията $f(x)$ е два пъти непрекъснато диференцируема в $[a,b]$, нека производната ѝ $f'(x)$ е монотонна в $[a,b]$ и*

$$|f'(x)| \ge \lambda > 0 \qquad \text{при} \qquad x \in [a,b]. \tag{237}$$

Тогава за интеграла I, определен чрез (236) *е изпълнено*

$$|I| \le \lambda^{-1}. \tag{238}$$

Доказателство. Тъй като по условие имаме $f'(x) \ne 0$, то можем да запишем

$$I = \int_a^b \frac{1}{f'(x)}\,f'(x)\,e(f(x))\,dx = \frac{1}{2\pi i}\int_a^b \frac{1}{f'(x)}\,d\,e(f(x)).$$

Сега интегрираме по части и получаваме

$$I = \frac{1}{2\pi i}\left(\frac{e(f(b))}{f'(b)} - \frac{e(f(a))}{f'(a)} - J\right), \tag{239}$$

където

$$J = \int_a^b e(f(x))\,d\,\frac{1}{f'(x)} = -\int_a^b e(f(x))\,\frac{f''(x)}{f'(x)^2}\,dx. \tag{240}$$

От (237) и (239) получаваме

$$|I| \le \frac{1}{2\pi}\left(\frac{1}{|f'(b)|} + \frac{1}{|f'(a)|} + |J|\right) \le \frac{1}{2\pi}\left(\frac{2}{\lambda} + |J|\right). \tag{241}$$

Остава да оценим интеграла J. От (240) имаме

$$|J| \le F \qquad \text{където} \qquad F = \int_a^b \frac{|f''(x)|}{f'(x)^2}\,dx. \tag{242}$$

Тъй като по условие функцията $f'(x)$ е монотонна в $[a,b]$, то $f''(x)$ не си променя знака в този интервал. Но тогава функцията $f''(x)f'(x)^{-2}$ също не си мени знака в $[a,b]$, откъдето следва, че

$$F = \left|\int_a^b \frac{f''(x)}{f'(x)^2}\,dx\right|.$$

От горната формула, от теоремата на Нютон–Лайбниц и от условието (237) следва

$$F = \left| \int_a^b \frac{d\,(f'(x))}{f'(x)^2} \right| = \left| - \int_a^b d\left(\frac{1}{f'(x)}\right) \right| = \left| \frac{1}{f'(a)} - \frac{1}{f'(b)} \right| \le \frac{1}{|f'(a)|} + \frac{1}{|f'(b)|} \le \frac{2}{\lambda}.$$

От последната формула, (241) и (242) следва (238).

□

В следващата лема ще оценим експоненциалния интеграл I, определен чрез (236) при условие, че втората производна $f''(x)$ е „голяма". Имаме

Лема 4.15. *Нека функцията $f(x)$ е два пъти непрекъснато диференцируема в $[a, b]$ и нека*

$$|f''(x)| \ge \lambda > 0 \qquad \textit{при} \qquad x \in [a, b]. \tag{243}$$

Тогава за интеграла I, определен чрез (236)*, е изпълнено*

$$|I| \le 4\lambda^{-\frac{1}{2}}. \tag{244}$$

Доказателство. Представяме интервала $[a, b]$ във вида

$$[a, b] = E_1 \cup E_2, \tag{245}$$

където

$$E_1 = \{x \in [a, b] \ : \ |f'(x)| \ge \mu\}, \qquad E_2 = \{x \in [a, b] \ : \ |f'(x)| < \mu\} \tag{246}$$

и където $\mu > 0$ е параметър, който ще изберем по-късно. От условието (243) следва, че $f'(x)$ е или строго растяща, или строго намаляваща в $[a, b]$. Тогава множеството E_1 се състои най-много от два интервала и, като за всеки от тях приложим Лема 4.14, получаваме

$$\left| \int_{E_1} e(f(x))\, dx \right| \le \frac{2}{\mu}. \tag{247}$$

Да разгледаме сега множеството E_2. Ясно е, че то е или празно, или е интервал с краища u и v, където $a \le u < v \le b$. Във втория случай прилагаме теоремата за крайните нараствания и получаваме, че $f'(v) - f'(u) = f''(\xi)(v - u)$ за някое $\xi \in (u, v)$. Но от определението на E_2, зададено чрез (246), следва, че $|f'(u)| \le \mu$, $|f'(v)| \le \mu$. Тогава, като вземем предвид условието (243) получаваме

$$v - u = \frac{|f'(v) - f'(u)|}{|f''(\xi)|} \le \frac{|f'(v)| + |f'(u)|}{\lambda} \le \frac{2\mu}{\lambda}.$$

Оттук следва, че

$$\left| \int_{E_2} e(f(x))\, dx \right| \le \int_{E_2} dx = v - u \le \frac{2\mu}{\lambda}. \tag{248}$$

Очевидно последната оценка е вярна и когато $E_2 = \emptyset$.

От (236), (245), (247) и (248) следва оценката

$$|I| \le \left| \int\limits_{E_1} e(f(x))\,dx \right| + \left| \int\limits_{E_2} e(f(x))\,dx \right| \le \frac{2}{\mu} + \frac{2\mu}{\lambda}.$$

Сега, като положим $\mu = \sqrt{\lambda}$, получаваме (244).

$\square$

Сега вече сме в състояние да докажем важната теорема на Ван-дер-Корпут, която играе основна роля в при решаването на много задачи от аналитичната теория на числата.

Теорема 4.16 (Ван-дер-Корпут). *Нека функцията $f(x)$ е реалнозначна и два пъти непрекъснато диференцируема в интервала $[a,b]$. Нека*

$$b - a \ge 10, \qquad \mu \ge 1, \qquad \rho > 0 \tag{249}$$

и

$$0 < \rho \le |f''(x)| \le \mu\rho \qquad \textit{при} \qquad x \in [a,b]. \tag{250}$$

Тогава за сумата

$$S = \sum_{a<n\le b} e(f(n)), \tag{251}$$

е в сила оценката

$$S \ll \mu(b-a)\rho^{\frac{1}{2}} + \rho^{-\frac{1}{2}}, \tag{252}$$

като константата в знака $\ll$ е абсолютна.

Забележка. В приложенията μ винаги е константа, така че обикновено се пропуска в записа на дясната страна на (252).

Доказателство. Без ограничение на общността можем да считаме, че $0 < \rho < \frac{1}{10}$. Наистина, ако $\rho \ge \frac{1}{10}$, то изразът в дясната страна на (252) е по-голям от $(b-a)/100$ и тогава (252) е следствие от тривиалната оценка за S.

Можем да считаме също, че

$$0 < \rho \le f''(x) \le \mu\rho \qquad \text{при} \qquad x \in [a,b]. \tag{253}$$

Наистина, нека сме доказали теоремата в този случай. Тогава, ако е изпълнено

$$0 < \rho \le -f''(x) \le \mu\rho \qquad \text{при} \qquad x \in [a,b],$$

разглеждаме сума аналогична на S, но с функция $-f(x)$ вместо с $f(x)$. Тъй като при тази промяна модулът на S не се изменя, то оценката (252) отново е вярна.

По-нататък, можем да считаме, че a и b са числа от вида $k + \frac{1}{2}$, $k \in \mathbb{Z}$. Наистина, ако оценката (252) е доказана при това предположение, то в общия случай заменяме

a и b съответно с числа $a_1, b_1 \in [a,b]$, които са от вида $k+\frac{1}{2}$, $k \in \mathbb{Z}$ и за които $|a-a_1|, |b-b_1| \le \frac{1}{2}$. При това сумата S се променя с величина $O(1)$, която се мажорира от израза в дясната страна на (252).

Сега условията от Лема 4.13 са изпълнени, следователно имаме

$$S = \sum_{f'(a)-1\le n\le f'(b)+1} \int\limits_a^b e\left(f(x)-nx\right)\,dx + O\Big(\log(f'(b)-f'(a)+2)\Big)$$

$$\ll \sum_{f'(a)-1\le n\le f'(b)+1} \left|\int\limits_a^b e\left(f(x)-nx\right)\,dx\right| + \log(f'(b)-f'(a)+2). \tag{254}$$

За да оценим интегралите в горната формула, прилагаме Лема 4.15 и виждаме, че

$$\left|\int\limits_a^b e\left(f(x)-nx\right)\,dx\right| \le 4\rho^{-\frac{1}{2}}.$$

Като заместим последната оценка в (254), получаваме

$$S \ll \big(f'(b)-f'(a)+2\big)\,\rho^{-\frac{1}{2}} + \log\big(f'(b)-f'(a)+2\big) \ll \big(f'(b)-f'(a)+2\big)\,\rho^{-\frac{1}{2}}$$

$$\ll \big(f'(b)-f'(a)\big)\,\rho^{-\frac{1}{2}} + \rho^{-\frac{1}{2}}. \tag{255}$$

Но от теоремата за крайните нараствания следва, че

$$f'(b)-f'(a) = f''(\eta)(b-a)$$

за някое $\eta \in (a,b)$. Тогава, като приложим (253), виждаме, че

$$f'(b)-f'(a) \le \mu\rho(b-a).$$

Заместваме последната оценка в (255) и получаваме (252).

$\square$

4.8 Оценка на сума от стойности на функцията $\rho(t)$

В настоящия параграф ще оценяваме суми от вида

$$T = \sum_{a<n\le b} \rho\left(f(n)\right), \tag{256}$$

където $f(x)$ е реалнозначна функция, определена в интервала $[a,b]$. Както се убедихме в параграфи 4.4 и 4.5, величините $\Delta_K(R)$ и $\Delta_L(R)$ се изразяват чрез суми от такъв тип. От Лема 2.3 (2) и от неравенството на триъгълника следва тривиалната оценка

$$|T| \le \frac{1}{2}\left([b]-[a]\right), \tag{257}$$

но за приложенията обикновено тя не е достатъчно точна. Ако обаче се използуват някои специфични свойства на функцията $f(x)$, то в много случаи е възможно получаването на оценка, много по-силна от (257). Ще видим, че оценяването на сумата T се свежда до оценяването на експоненциални суми. Това ще ни даде възможност, ако са налице определени условия за функцията $f(x)$, да се възползуваме от Теорема 4.16 и по този начин да оценим нетривиално сумата T.

Теорема 4.17. *Нека $f(x)$ е реалнозначна и два пъти непрекъснато диференцируема в $[a,b]$, нека*

$$b-a\geq 10, \qquad \mu\geq 1, \qquad \rho>0 \tag{258}$$

и

$$0<\rho\leq |f''(x)|\leq \mu\rho \qquad \text{при} \qquad x\in[a,b]. \tag{259}$$

Тогава за сумата T, определена чрез (256)*, е в сила оценката*

$$T \ll \left(\mu\,(b-a)\,\rho^{\frac{1}{3}}+\rho^{-\frac{1}{2}}\right)\log\left(\rho^{-1}+2\right)\,. \tag{260}$$

Забележка. В приложенията μ винаги е константа, така че обикновено в записа на дясната страна на (260) тя се пропуска.

Доказателство. Можем да считаме, че

$$0<\rho<\frac{1}{10}, \tag{261}$$

тъй като при $\rho\geq\frac{1}{10}$ оценката (260) е следствие от тривиалната оценка $T\ll b-a$.

Като използуваме Лема 4.11 записваме функцията $\rho(t)$ във вида

$$\rho(t)=\sum_{1\leq|h|\leq M}\frac{e(ht)}{2\pi ih}+O\left(\min\left(1,\frac{1}{M||t||}\right)\right), \tag{262}$$

където $M\geq 2$ е параметър, който по-късно ще изберем по подходящ начин като функция на ρ. Тогава от (256) и (262) следва

$$T=\sum_{a<n\leq b}\left(\sum_{1\leq|h|\leq M}\frac{e(hf(n))}{2\pi ih}+O\left(\min\left(1,\frac{1}{M||f(n)||}\right)\right)\right)$$

$$=\sum_{1\leq|h|\leq M}\frac{1}{2\pi ih}\,S_h+O\left(\Sigma\right), \tag{263}$$

където

$$S_h=\sum_{a<n\leq b}e\left(hf(n)\right) \tag{264}$$

и

$$\Sigma=\sum_{a<n\leq b}\min\left(1,\frac{1}{M||f(n)||}\right). \tag{265}$$

Да разгледаме сумата Σ. От (264), (265) и от Лема 4.12 получаваме

$$\Sigma = \sum_{a<n\le b}\sum_{h\in\mathbb{Z}} b(h)\, e\,(hf(n)) = \sum_{h\in\mathbb{Z}} b(h)\, S_h, \tag{266}$$

където

$$b(h) \ll \frac{\log M}{M} \quad \text{за всяко } h\,, \qquad b(h) \ll \frac{M}{h^2} \quad \text{при } h\neq 0. \tag{267}$$

Да отбележим, че безкрайният ред в (266) е абсолютно сходящ вследствие на второто от неравенствата (267). Оттук получаваме

$$\Sigma \ll \sum_{h\in\mathbb{Z}} |b(h)|\,|S_h| \ll \frac{\log M}{M}\sum_{|h|\le M}|S_h| + M\sum_{M<|h|}\frac{1}{h^2}\,|S_h|. \tag{268}$$

За сумата (264) очевидно е изпълнена тривиалната оценка

$$|S_h| \ll b-a, \tag{269}$$

която използваме при $h=0$ и при $|h|>M^2$. Като използваме (268) и като вземем предвид неравенството

$$\sum_{n>x} n^{-2} \ll x^{-1},$$

което е частен случай на Лема 2.6 (2), получаваме

$$\Sigma \ll \frac{\log M}{M}\,(b-a) + \frac{\log M}{M}\sum_{1\le|h|\le M}|S_h| + M\sum_{M<|h|\le M^2}\frac{1}{h^2}\,|S_h|.$$

От (264) следва, че $|S_h| = |S_{-h}|$, така че в горната формула можем да сумираме само по естествените числа h и това ще доведе само до промяна на константата в знака $\ll$. Тогава намираме, че

$$\Sigma \ll \frac{\log M}{M}\,(b-a) + \frac{\log M}{M}\sum_{h\le M}|S_h| + M\sum_{M<h\le M^2}\frac{1}{h^2}\,|S_h|$$

$$\ll \frac{\log M}{M}\,(b-a) + \log M\sum_{h\le M}\frac{1}{h}\,|S_h| + M\sum_{M<h\le M^2}\frac{1}{h^2}\,|S_h|. \tag{270}$$

От (263) и (270) получаваме

$$T \ll \frac{\log M}{M}\,(b-a) + \log M\sum_{h\le M}\frac{1}{h}\,|S_h| + M\sum_{M<h\le M^2}\frac{1}{h^2}\,|S_h|. \tag{271}$$

Сега ще оценим S_h при $1\le h\le M^2$ като използваме Теорема 4.16. Ако $F(x) = hf(x)$, то от (259) следва

$$h\rho \le |F''(x)| \le \mu h\rho \qquad \text{при} \qquad x\in[a,b].$$

Тогава от Теорема 4.16 получаваме

$$S_h \ll \mu(b-a)(h\rho)^{\frac{1}{2}} + (h\rho)^{-\frac{1}{2}}.$$

От тази оценка и от Лема 2.6 (1) следва, че

$$\sum_{h\le M} \frac{1}{h}\,|S_h| \ll \mu(b-a)\,\rho^{\frac{1}{2}} \sum_{h\le M} h^{-\frac{1}{2}} + \rho^{-\frac{1}{2}} \sum_{h\le M} h^{-\frac{3}{2}}$$

$$\ll \mu(b-a)\,\rho^{\frac{1}{2}} M^{\frac{1}{2}} + \rho^{-\frac{1}{2}}. \tag{272}$$

Аналогично, като използуваме Лема 2.6 (2) намираме, че

$$\sum_{M<h\le M^2} \frac{1}{h^2}\,|S_h| \ll \mu(b-a)\,\rho^{\frac{1}{2}} \sum_{M<h\le M^2} h^{-\frac{3}{2}} + \rho^{-\frac{1}{2}} \sum_{M<h\le M^2} h^{-\frac{5}{2}}$$

$$\ll \mu(b-a)\,\rho^{\frac{1}{2}} M^{-\frac{1}{2}} + \rho^{-\frac{1}{2}} M^{-\frac{3}{2}}. \tag{273}$$

От (271) – (273) следва

$$T \ll \left(\frac{b-a}{M} + \mu(b-a)\,\rho^{\frac{1}{2}} M^{\frac{1}{2}} + \rho^{-\frac{1}{2}}\right) \log M. \tag{274}$$

Сега избираме M така, че първите две събираеми в скобите в дясната част на (274) да бъдат по порядък равни — тогава оценката за T ще бъде най-точна. При това не отчитаме присъствието на величината μ, тъй като в приложенията тя винаги е константа и не оказва съществено. И така, определяме M от равенството

$$(b-a)\,M^{-1} = (b-a)\,\rho^{\frac{1}{2}}\,M^{\frac{1}{2}},$$

откъдето

$$M = \rho^{-\frac{1}{3}}. \tag{275}$$

Тъй като считаме, че е изпълнено условието (261), то така определеното M удовлетворява условието $M \ge 2$. От (274) и (275) получаваме (260), с което теоремата е доказана.

$\square$

4.9 Доказателство на Теорема 4.2

Ще приложим Теорема 4.17, за да оценим величината $\Delta_K^*(R)$, определена чрез (185). Тя съвпада със сумата T, зададена с равенството (256), където

$$a = 0, \qquad b = \sqrt{\frac{R}{2}}, \qquad f(x) = \sqrt{R - x^2}.$$

Имаме

$$f'(x) = -x\,(R - x^2)^{-\frac{1}{2}}, \qquad f''(x) = -R\,(R - x^2)^{-\frac{3}{2}}$$

Ясно е, че

$$R^{-\frac{1}{2}} \leq |f''(x)| \leq 2^{\frac{3}{2}} R^{-\frac{1}{2}} \qquad \text{при} \quad 0 \leq x \leq \sqrt{\frac{R}{2}}.$$

Тогава, ако положим

$$\rho = R^{-\frac{1}{2}}, \qquad \mu = 2^{\frac{3}{2}}$$

виждаме, че условията на Теорема 4.17 са удовлетворени. Следователно

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

Остава да приложим (184) и получаваме

$$\Delta_K(R) \ll R^{\frac{1}{3}} \log R,$$

с което Теорема 4.2 е доказана.

□

4.10 Доказателство на Теорема 4.5

Да разгледаме величината $\Delta_L^*(R)$, определена чрез (198). Тя е сума от вида (256) с функция

$$f(x) = \frac{R}{x}. \tag{276}$$

В този случай обаче директното прилагане та Теорема 4.17 не е удачно, тъй като втората производна

$$f''(x) = \frac{2R}{x^3} \tag{277}$$

варира в много широки граници, когато x пробягва числата от интервала $\left(0, \sqrt{R}\,\right]$. За да избегнем това неудобство, разделяме $\Delta_L^*(R)$ на части по следния начин:

$$\Delta_L^*(R) = \sum_{i=1}^{i_0} \Delta_i + \Delta^{(0)}, \tag{278}$$

където

$$\Delta_i = \sum_{\frac{\sqrt{R}}{2^i} < n \leq \frac{\sqrt{R}}{2^{i-1}}} \rho\left(\frac{R}{n}\right), \qquad \Delta^{(0)} = \sum_{n \leq \frac{\sqrt{R}}{2^{i_0}}} \rho\left(\frac{R}{n}\right), \tag{279}$$

а числото i_0 се определя от условията

$$\frac{\sqrt{R}}{2^{i_0}} < R^{\frac{1}{3}} \leq \frac{\sqrt{R}}{2^{i_0-1}}. \tag{280}$$

От (280) очевидно следва

$$i_0 \ll \log R. \tag{281}$$

Величината $\Delta^{(0)}$ оценяваме тривиално. Като използуваме Лема 2.3 (2), неравенството на триъгълника и първото неравенство от (280) получаваме

$$\Delta^{(0)} \ll R^{\frac{1}{3}}. \tag{282}$$

Да разгледаме сега Δ_i при $1 \le i \le i_0$. Прилагаме Теорема 4.17 при

$$a = R^{\frac{1}{2}}\, 2^{-i}, \qquad b = R^{\frac{1}{2}}\, 2^{-i+1}$$

и с функцията $f(x)$, определена чрез (276). От (277) следва, че

$$2^{3i-2} R^{-\frac{1}{2}} \le f''(x) \le 2^{3i+1} R^{-\frac{1}{2}} \qquad \text{при} \qquad \sqrt{R}\, 2^{-i} \le x \le \sqrt{R}\, 2^{-i-1}.$$

Следователно, ако положим

$$\rho = 2^{3i-2} R^{-\frac{1}{2}}, \qquad \mu = 8,$$

то всички условия на Теорема 4.17 са налице и получаваме

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

От последната формула, (278), (281) и (282) следва

$$\Delta_L^*(R) \ll R^{\frac{1}{3}} \log^2 R.$$

Остава да вземем предвид (197) и получаваме (182). С това теоремата е доказана. $\square$

5 Разпределение на простите числа

5.1 Формулировка на теоремата на Чебишев

Ще въведем една от най-важните функции в теорията на числата.

Определение 5.1. *За всяко $x \geq 2$ означаваме с $\pi(x)$ броя на простите числа ненадминаващи x, т.е.*

$$\pi(x) = \sum_{p \leq x} 1. \tag{283}$$

Например, тъй като простите числа ненадминаващи 10 са 2, 3, 5, и 7, то $\pi(10) = 4$.

Още Гаус се е занимавал с намиране на приближения на $\pi(x)$ чрез познати функции. Пресмятанията, които той е извършил, са го довели до мисълта, че ако вземем „случайно" естествено число, ненадминаващо x, то „вероятността" това число да е просто е приблизително равна на $(\log x)^{-1}$. Поради това Гаус е предположил, че за достатъчно големи x стойността на $\pi(x)$ е приближено равна на $x/\log x$. С тази задача впоследствие са се занимавали Льожандър, Риман, Чебишев, Адамар, Вале-Пусен, Х.Вейл, Виноградов и други знаменити математици.

В настоящия параграф ще се занимаем с теоремата на Чебишев, според която съществуват константи $c_1, c_2 > 0$ такива, че при $x \geq 2$ е изпълнено

$$c_1 \frac{x}{\log x} \leq \pi(x) \leq c_2 \frac{x}{\log x}.$$

Ще докажем също известните *теореми на Мертенс*, които са тясно свързани с разпределението на простите числа.

По-късно ще въведем дзета-функцията на Риман и изучим някои от свойствата ѝ. Това ще ни даде възможност да докажем Теорема 5.34, която е известна като *асимптотичен закон за разпределението на простите числа* и гласи, че

$$\lim_{x \to \infty} \frac{\pi(x)}{x/\log x} = 1.$$

Наред с $\pi(x)$, в теорията за разпределението на простите числа важна роля играят функциите на Чебишев $\theta(x)$ и $\psi(x)$, зададени съответно чрез

Определение 5.2. *За всяко $x \geq 2$ означаваме*

$$\theta(x) = \sum_{p \leq x} \log p. \tag{284}$$

Определение 5.3. *За всяко $x \geq 2$ означаваме*

$$\psi(x) = \sum_{n \leq x} \Lambda(n). \tag{285}$$

Например, имаме

$$\begin{aligned}\theta(10) &= \log 2 + \log 3 + \log 5 + \log 7,\\ \psi(10) &= \log 2 + \log 3 + \log 2 + \log 5 + \log 7 + \log 2 + \log 3.\end{aligned}$$

Чебишев е забелязал, че функциите $\pi(x)$, $\theta(x)$ и $\psi(x)$ са тясно свързани и че намирането на точния порядък при големи x на някоя от тях води до намирането на порядъците и на другите две. Той е доказал следната

Теорема 5.4 (Чебишев)**.** *При $x \ge 2$ е изпълнено*

$$\pi(x) \asymp \frac{x}{\log x}, \tag{286}$$

$$\theta(x) \asymp x, \tag{287}$$

$$\psi(x) \asymp x. \tag{288}$$

Доказателството на тази теорема се получава като следствие от няколко леми, които последователно ще докажем. Ще отбележим, че Чебишев установява по-силна версия на Теорема 5.4 с явни стойности на константите в знаците $\asymp$. С този въпрос, обаче, в настоящите записки няма да се занимаваме.

5.2 Оценки отгоре за $\pi(x)$, $\theta(x)$ и $\psi(x)$

В следващата лема ще видим, че функциите $\theta(x)$ и $\psi(x)$ се отличават малко едно от друга.

Лема 5.5. *В сила е асимптотичната формула*

$$\psi(x) = \theta(x) + O\left(\sqrt{x}\, \log^2 x\right). \tag{289}$$

Доказателство. Според определения (25), (284), (285) имаме

$$\psi(x) = \sum_{n \le x} \Lambda(n) = \sum_{\substack{k\in\mathbb{N}\,,\, p \\ p^k \le x}} \log p = \theta(x) + \Delta(x),$$

където

$$\Delta(x) = \sum_{\substack{k\ge 2\,,\, p \\ p^k \le x}} \log p.$$

От условията за k и p в последната сума следва, че $p \le \sqrt{x}$, откъдето $\log p \le \frac{1}{2} \log x$. Имаме също $2^k \le p^k \le x$, т.е. $k \le \frac{\log x}{\log 2}$. Тогава

$$0 \le \Delta(x) \le \frac{1}{2} \log x \sum_{2 \le k \le \frac{\log x}{\log 2}} \sum_{p \le \sqrt{x}} 1 \ll \sqrt{x}\, \log^2 x,$$

с което лемата е доказана.

$\square$

Да отбележим, че с помощта на малко по-прецизни изчисления може да се установи, че остатъчният член в (289) е всъщност равен на $O(\sqrt{x})$.

Следващата лема ни казва, че ако знаем порядъка на една от функциите $\theta(x)$, $\pi(x)$ можем да направим заключение и за порядъка на другата.

Лема 5.6. *За всяко $x \geq 2$ са изпълнени неравенствата*

$$\frac{1}{2}(\pi(x) - \sqrt{x}) \log x \leq \theta(x) \leq \pi(x) \log x$$

Доказателство. Очевидно е, че

$$\theta(x) = \sum_{p \leq x} \log p \leq \log x \sum_{p \leq x} 1 = \pi(x) \log x.$$

От друга страна имаме

$$\theta(x) \geq \sum_{\sqrt{x} < p \leq x} \log p \geq \log \sqrt{x} \sum_{\sqrt{x} < p \leq x} 1 \geq \frac{1}{2} \left(\pi(x) - \sqrt{x} \right) \log x,$$

с което лемата е доказана.

$\square$

Един от основните резултати, водещи до доказателството на Теорема 5.4 следната лема, в която функцията $\theta(x)$ се оценява отгоре.

Лема 5.7. *При $x \geq 2$ е изпълнено*

$$\theta(x) \leq x \log 4. \tag{290}$$

Доказателство. Достатъчно е да докажем, че за всяко $n \in \mathbb{N}$ е изпълнено

$$\prod_{p \leq n} p \leq 4^n. \tag{291}$$

Наистина, ако това неравенство е доказано, то при $x \in \mathbb{R}$, $x \geq 2$ имаме

$$\prod_{p \leq x} p = \prod_{p \leq [x]} p \leq 4^{[x]} \leq 4^x.$$

Сега, като логаритмуваме и използуваме (284), получаваме (290).

Да пристъпим към доказателството на (291). При $n = 1$ и при $n = 2$ верността на това неравенство е очевидна. Допускаме, че $n > 2$ и че неравенството е изпълнено за числата по-малки от n.

Ако n е четно, то не може да бъде просто и, като вземем предвид нашето допускане, получаваме

$$\prod_{p \leq n} p = \prod_{p \leq n-1} p \leq 4^{n-1} < 4^n.$$

Сега да разгледаме случая, когато n е нечетно. Полагаме $n = 2m + 1$, където $m \geq 1$ е цяло число. Да разгледаме биномния коефициент

$$M = \binom{2m+1}{m} = \frac{(2m+1)(2m)(2m-1)\dots(m+2)}{m!}. \tag{292}$$

Очевидно числителят на дробта в дясната страна на (292) се дели на числото

$$N = \prod_{m+1<p\leq 2m+1} p, \tag{293}$$

откъдето $N \mid m!M$. Но тъй като $(N, m!) = 1$, то от Лема 3.14 следва, че $N \mid M$. Оттук получаваме

$$N \leq M. \tag{294}$$

От друга страна, имаме

$$2^{2m+1} = \sum_{k=0}^{2m+1} \binom{2m+1}{k} \geq \binom{2m+1}{m} + \binom{2m+1}{m+1} = 2M,$$

откъдето $M \leq 4^m$. От последното неравенство и от (294) следва

$$N \leq 4^m. \tag{295}$$

От индукционното допускане, (293) и (295) получаваме

$$\prod_{p\leq n} p = N \prod_{p\leq m+1} p \leq 4^m \cdot 4^{m+1} = 4^n,$$

с което неравенството (291) е доказано.

□

И така, вече доказахме оценката отгоре от Теорема 5.4 за функцията $\theta(x)$ (и то с конкретна константа в знака $\ll$). Това ни дава възможност лесно да оценим отгоре и функциите $\pi(x)$ и $\psi(x)$.

Лема 5.8. *При $x \geq 2$ са в сила оценките*

$$\pi(x) \ll \frac{x}{\log x}, \qquad \psi(x) \ll x.$$

Доказателство. Оценката за $\pi(x)$ следва от Лема 5.6 и Лема 5.7, а оценката за $\psi(x)$ съответно от Лема 5.5 и Лема 5.7.

□

5.3 Формули на Мертенс

Ще докажем няколко важни асимптотични формули, известни като *формули на Мертенс*. Първото от тях е приведена в следната

Лема 5.9 (Мертенс)**.** *При* $x \geq 2$ *е изпълнено*

$$\sum_{n \leq x} \frac{\Lambda(n)}{n} = \log x + O\left(1\right). \tag{296}$$

Доказателство. Да разгледаме величината

$$S = \sum_{n \leq x} \log n.$$

Според Лема 2.6 (4) имаме

$$S = x \log x + O(x). \tag{297}$$

От друга, страна от Лема 3.42 следва, че

$$S = \sum_{n \leq x} \sum_{d \mid n} \Lambda(d) = \sum_{d \leq x} \Lambda(d) \sum_{\substack{n \leq x \\ n \equiv 0 \pmod d}} 1 = \sum_{d \leq x} \Lambda(d) \left[\frac{x}{d}\right].$$

Оттук и от равенството (2) намираме

$$S = \sum_{d \leq x} \Lambda(d) \left(\frac{x}{d} - \left\{\frac{x}{d}\right\}\right) = x \sum_{d \leq x} \frac{\Lambda(d)}{d} - S_1, \tag{298}$$

където

$$S_1 = \sum_{d \leq x} \Lambda(d) \left\{\frac{x}{d}\right\}.$$

Ясно е, че от горната формула и от Лема 5.8 следва

$$0 \leq S_1 \leq \sum_{d \leq x} \Lambda(d) = \psi(x) \ll x. \tag{299}$$

От (297) – (299) намираме, че

$$x \log x + O(x) = x \sum_{d \leq x} \frac{\Lambda(d)}{d}$$

и като разделим на x получаваме (296).

□

От горната лема лесно се получава

Лема 5.10 (Мертенс)**.** *При* $x \geq 2$ *е изпълнено*

$$\sum_{p \leq x} \frac{\log p}{p} = \log x + O\left(1\right). \tag{300}$$

Доказателство. От определението (25) на функцията на Манголд следва, че

$$\sum_{n\le x}\frac{\Lambda(n)}{n}=\sum_{\substack{k\in\mathbb{N},\,p\\ p^k\le x}}\frac{\log p}{p^k}=\sum_{p\le x}\frac{\log p}{p}+\Delta(x),$$

където

$$\Delta(x)=\sum_{\substack{k\ge 2,\,p\\ p^k\le x}}\frac{\log p}{p^k}$$

Имаме

$$0\le\Delta(x)\le\sum_{p\le x}\log p\sum_{k=2}^{\infty}\frac{1}{p^k}=\sum_{p\le x}\frac{\log p}{p(p-1)}\le\sum_{n=2}^{\infty}\frac{\log n}{n(n-1)}.$$

Тъй като последният безкраен ред е сходящ, намираме, че $\Delta(x)=O(1)$, с което лемата е доказана.

$\square$

Третата формула на Мертенс е дадена в следната

Лема 5.11 (Мертенс)**.** *При $x\ge 2$ е изпълнено*

$$\sum_{p\le x}\frac{1}{p}=\log\log x+c+O\left(\frac{1}{\log x}\right), \tag{301}$$

където c е константа.

Доказателство. Да означим с S сумата от лявата страна на (301). Като използваме преобразованието на Абел (Лема 2.1), получаваме

$$S=\sum_{3/2<p\le x}\frac{\log p}{p}\cdot\frac{1}{\log p}=\frac{C(x)}{\log x}-\int\limits_2^x C(t)\left(\frac{1}{\log t}\right)'dt,$$

където

$$C(t)=\sum_{p\le t}\frac{\log p}{p}\,.$$

Но от Лема 5.10 имаме

$$C(t)=\log t+\Delta(t)\,,\qquad \Delta(t)=O(1) \tag{302}$$

и тогава

$$\begin{aligned}S&=\frac{\log x+\Delta(x)}{\log x}-\int\limits_2^x\big(\log t+\Delta(t)\big)\left(\frac{1}{\log t}\right)'dt\\&=1+\frac{\Delta(x)}{\log x}+\int\limits_2^x\frac{dt}{t\log t}+\int\limits_2^x\frac{\Delta(t)}{t\log^2 t}\,dt.\end{aligned} \tag{303}$$

От оценката за $\Delta(t)$ в (302) следва, че интегралът $\int_2^\infty \frac{\Delta(t)}{t\log^2 t}\,dt$ е абсолютно сходящ. Тогава от (303) следва

$$S = \log\log x + c + \delta(x),$$

където

$$c = 1 - \log\log 2 + \int_2^\infty \frac{\Delta(t)}{t\log^2 t}dt\,, \qquad \delta(x) = \frac{\Delta(x)}{\log x} - \int_x^\infty \frac{\Delta(t)}{t\log^2 t}\,dt.$$

От горната формула и (302) следва

$$\delta(x) \ll \frac{1}{\log x} + \int_x^\infty \frac{dt}{t\log^2 t} \ll \frac{1}{\log x},$$

с което лемата е доказана.

□

От последната лема следва, че безкрайният ред $\sum_p p^{-1}$, където сумирането е по всички прости числа, е разходящ. Този факт е бил установен още от Ойлер, който е получил оценката $\sum_{p\le x} p^{-1} \gg \log\log x$. По този начин Ойлер е намерил ново доказателство на теоремата на Евклид за безкрайността на множеството от всички прости числа.

Последната от формулите на Мертенс е приведена в следната

Лема 5.12 (Мертенс)**.** *При* $x \ge 2$ *е изпълнено*

$$\prod_{p\le x}\left(1 - \frac{1}{p}\right) = \frac{c_1}{\log x}\left(1 + O\left(\frac{1}{\log x}\right)\right), \tag{304}$$

където $c_1 > 0$ *е константа.*

Доказателство. Означаваме с P произведението в лявата част на (304). Като използваме, че $\log(1+t) = t + O(t^2)$ при $|t| \le 1/2$, намираме

$$\log P = \sum_{p\le x}\log\left(1 - \frac{1}{p}\right) = \sum_{p\le x}\left(-\frac{1}{p} + \delta_p\right) = -\sum_{p\le x}\frac{1}{p} + \sum_{p\le x}\delta_p, \tag{305}$$

като

$$\delta_p = O\big(p^{-2}\big). \tag{306}$$

От оценката (306) следва, че безкрайният ред $\sum_p \delta_p$, където сумирането е по всички прости числа, е абсолютно сходящ. Като означим сумата му с α и като вземем предвид (306) и Лема 2.6 (2), намираме

$$\sum_{p\le x}\delta_p = \alpha - \sum_{p>x}\delta_p = \alpha + O\Big(\sum_{p>x}|\delta_p|\Big) = \alpha + O\Big(\sum_{n>x}\frac{1}{n^2}\Big) = \alpha + O\Big(\frac{1}{x}\Big) \tag{307}$$

Използваме (305), (307) и Лема 5.11 и получаваме

$$\log P = -\sum_{p\le x}\frac{1}{p} + \alpha + O\Big(\frac{1}{x}\Big) = -\log\log x - c + \alpha + \Delta(x),$$

като
$$\Delta(x) = O\left(\frac{1}{\log x}\right). \tag{308}$$
Тогава
$$P = e^{\log P} = e^{-\log\log x - c + \alpha + \Delta(x)} = \frac{c_1}{\log x}\, e^{\Delta(x)},$$
където $c_1 = e^{-c+\alpha} > 0$ е константа. Тъй като $e^t = 1 + O(|t|)$, когато t е в околност нулата, от (308) следва
$$e^{\Delta(x)} = 1 + O\Big(\frac{1}{\log x}\Big),$$
с което лемата е доказана.

□

Може да се докаже, че константата c_1 от формула (304) е равна на $e^{-\gamma}$, където γ е константата на Ойлер.

5.4 Завършване на доказателството на теоремата на Чебишев

В следващата лема са оценени отдолу функциите $\theta(x)$, $\psi(x)$ и $\pi(x)$, с което доказателството на Теорема 5.4 е завършено.

Лема 5.13. *При $x \geq 2$ са изпълнени оценките*
$$\theta(x) \gg x, \qquad \psi(x) \gg x, \qquad \pi(x) \gg \frac{x}{\log x}. \tag{309}$$

Доказателство. Ще започнем с изследването на $\theta(x)$. От Лема 5.10 следва, че съществува константа $A > 0$ такава, че
$$\left|\sum_{p\leq t} \frac{\log p}{p} - \log t\right| \leq A \qquad \text{при} \qquad t \geq 2. \tag{310}$$
Избираме число $\alpha \in (0,1)$, което удовлетворява условието
$$\log\frac{1}{\alpha} \geq 3A. \tag{311}$$
При $x \geq 2\alpha^{-1}$ разглеждаме сумата
$$S = \sum_{\alpha x < p \leq x} \frac{\log p}{p}. \tag{312}$$
Като вземем предвид (310) и неравенството на триъгълника виждаме, че
$$\begin{aligned}
\left|S - \log\frac{1}{\alpha}\right| &= \left|\left(\sum_{p\leq x}\frac{\log p}{p} - \log x\right) - \left(\sum_{p\leq \alpha x}\frac{\log p}{p} - \log(\alpha x)\right)\right| \\
&\leq \left|\sum_{p\leq x}\frac{\log p}{p} - \log x\right| + \left|\sum_{p\leq \alpha x}\frac{\log p}{p} - \log(\alpha x)\right| \\
&\leq 2A.
\end{aligned}$$

От (311) и от последното неравенство следва, че

$$S \geq A. \tag{313}$$

От друга страна, от (312) и от Определение 5.2 имаме

$$S \leq (\alpha x)^{-1} \sum_{\alpha x < p \leq x} \log p \leq (\alpha x)^{-1} \sum_{p \leq x} \log p = (\alpha x)^{-1}\, \theta(x). \tag{314}$$

Тогава от (313) и (314) получаваме

$$\theta(x) \geq \alpha A\, x \qquad \text{при} \qquad x \geq 2\alpha^{-1}.$$

Следователно, ако вместо αA вземем достатъчно малка константа $c > 0$, ще имаме

$$\theta(x) \geq cx \qquad \text{при} \qquad x \geq 2.$$

С това доказателството на първата от оценките (309) е завършено.

За да получим оценките отдолу за $\psi(x)$ и $\pi(x)$ от формула (309), остава да се възползуваме от Лема 5.5 и съответно Лема 5.6. С това лемата е доказана.

$\square$

5.5 Следствия

Лема 5.14. *Ако p_n означава n-тото просто число, то при $n \geq 2$ имаме*

$$p_n \asymp n \log n. \tag{315}$$

Доказателство. Очевидно имаме $n \leq p_n$. Тогава от Определение 5.1 и от теоремата на Чебишев (Теорема 5.4) следва

$$n = \pi\left(p_n\right) \ll \frac{p_n}{\log p_n} \ll \frac{p_n}{\log n},$$

откъдето

$$p_n \gg n \log n. \tag{316}$$

От друга страна, от Теорема 5.4 следва

$$n = \pi\left(p_n\right) \gg \frac{p_n}{\log p_n}. \tag{317}$$

Тогава за достатъчно големи n ще имаме $n \geq \sqrt{p_n}$, или все едно $p_n \leq n^2$. Оттук следва, че $\log p_n \ll \log n$ и, като вземем предвид (317) се убеждаваме, че

$$n \gg \frac{p_n}{\log n},$$

или все едно

$$p_n \ll n \log n. \tag{318}$$

От (316) и (318) следва (315).

$\square$.

Лема 5.15. *При всяко $n \in \mathbb{N}$ е изпълнено*

$$\varphi(n) \gg \frac{n}{\log\log(10n)}. \tag{319}$$

Доказателство. От Лема 3.40 следва, че ако различните прости делители на n са $q_1, \ldots, q_m$, като $q_1 < \cdots < q_m$, то

$$\frac{\varphi(n)}{n} = \prod_{i=1}^{m} \Big(1 - \frac{1}{q_i}\Big). \tag{320}$$

Нека $p_1 < p_2 < \cdots < p_m$ са първите m прости числа. Ясно е, че $p_i \le q_i$ при $1 \le i \le m$, откъдето $1 - \frac{1}{q_i} \ge 1 - \frac{1}{p_i}$ при $1 \le i \le m$. От (320) и от Лема 5.12 намираме

$$\frac{\varphi(n)}{n} \ge \prod_{i=1}^{m} \Big(1 - \frac{1}{p_i}\Big) = \prod_{p \le p_m} \Big(1 - \frac{1}{p}\Big) \gg \frac{1}{\log p_m}\,, \tag{321}$$

По-нататък, от Лема 5.14 следва, че

$$\log p_m \ll 1 + \log m. \tag{322}$$

Остава да оценим отгоре числото m. Имаме $n \ge q_1 \ldots q_m \ge 2^m$, откъдето $m \le \frac{\log n}{\log 2}$. Тогава

$$\log m \ll \log\log(10n). \tag{323}$$

Неравенството (319) е следствие от (321) – (323).

□

5.6 Редове на Дирихле

Предстои ни да видим как използването на по-сложна аналитична техника води до значително подобряване на резултатите за разпределението на простите числа, получени до момента. Ще започнем със следното

Определение 5.16. *Функционален ред от вида*

$$f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}, \tag{324}$$

където $s \in \mathbb{C}$ и $a_n \in \mathbb{C}, n = 1, 2, \ldots,$ се нарича ред на Дирихле.

Лема 5.17. *Нека редът на Дирихле (324) е сходящ в точката $s = s_0$ и нека е дадено произволно $\theta \in \big(0, \frac{\pi}{2}\big)$. Тогава този ред е равномерно сходящ в множеството*

$$\mathcal{K}(s_0;\theta) = \{s \in \mathbb{C} \ : \ s \ne s_0\,,\ |\arg(s - s_0)| \le \theta\,\}\,. \tag{325}$$

Доказателство. Достатъчно е да разгледаме случая $s_0 = 0$. Наистина, нека сме установили верността на твърдението в този случай. Тогава, за да докажем твърдението в общия случай, полагаме $w = s - s_0$ и разглеждаме реда

$$\sum_{n=1}^{\infty} \frac{a'_n}{n^w}, \qquad \text{където} \qquad a'_n = \frac{a_n}{n^{s_0}}.$$

И така, нека редът $\sum_{n=1}^{\infty} a_n$ е сходящ и нека $s = \sigma + i\tau \in K(0;\theta)$. Очевидно $\sigma > 0$ и, освен това

$$\frac{\sigma}{|s|} = \cos(\arg(s)) \geq \cos\theta. \tag{326}$$

Избираме $\varepsilon > 0$. Съществува $H \geq 1$ такова, че

$$\left| \sum_{M<n\leq N} a_n \right| \leq \varepsilon \cos\theta \qquad \text{при} \qquad H \leq M < N. \tag{327}$$

Тогава, ако $H \leq M < N$, то от преобразованието на Абел (Лема 2.1) следва

$$\sum_{M<n\leq N} \frac{a_n}{n^s} = N^{-s} \sum_{M<n\leq N} a_n - \int\limits_M^N \left(\sum_{M<n\leq t} a_n \right) \frac{d}{dt}\left(t^{-s}\right)\, dt$$

$$= N^{-s} \sum_{M<n\leq N} a_n + s \int\limits_M^N \left(\sum_{M<n\leq t} a_n \right) \frac{dt}{t^{s+1}}.$$

Като използваме неравенството на триъгълника, (326) и (327) виждаме, че равномерно по $s \in K(0,\theta)$ е изпълнено

$$\left| \sum_{M<n\leq N} \frac{a_n}{n^s} \right| \leq \left|N^{-s}\right| \left| \sum_{M<n\leq N} a_n \right| + |s| \int\limits_M^N \left| \sum_{M<n\leq t} a_n \right| \frac{dt}{|t^{s+1}|}$$

$$\leq \left(N^{-\sigma} + |s| \int\limits_M^N \frac{dt}{t^{\sigma+1}} \right) \varepsilon \cos\theta$$

$$= \left(N^{-\sigma} + \frac{|s|}{\sigma}\left(M^{-\sigma} - N^{-\sigma}\right) \right) \varepsilon \cos\theta$$

$$\leq \frac{|s|}{\sigma} M^{-\sigma}\, \varepsilon \cos\theta$$

$$\leq \varepsilon.$$

С това лемата е доказана.

$\square$

Лема 5.18. *Нека редът на Дирихле* (324) *е сходящ в точката* $s_0 = \sigma_0 + i\tau_0$. *Тогава той е равномерно сходящ във всяко компактно подмножество на полуравнината*

$$\mathcal{L}(\sigma_0) = \{s \in \mathbb{C} \ : \ Re(s) > \sigma_0\}\,.$$

Сумата му $f(s)$ *е аналитична функция в* $\mathcal{L}(\sigma_0)$ *и при всяко* $k \in \mathbb{N}$ *за нейната* k*-та производна имаме*

$$f^{(k)}(s) = \sum_{n=1}^{\infty} \frac{a_n\,(-\log n)^k}{n^s}.$$

Доказателство. Всяко компактно подмножество на $\mathcal{L}(s_0)$ се съдържа в множество от вида (325) за някое $\theta \in \left(0, \frac{\pi}{2}\right)$. Тогава от Лема 5.17 и от добре познатата теорема от теорията на аналитичните функции следва, че $f(s)$ е аналитична в $\mathcal{L}(s_0)$ и че производните ѝ се намират чрез почленно диференциране на реда (324).

$\square$

Лема 5.19. *За всеки ред на Дирихле е изпълнено точно едно от следните твърдения:*

(1) *Редът е сходящ за всяко* $s \in \mathbb{C}$.

(2) *Редът е разходящ за всяко* $s \in \mathbb{C}$.

(3) *Съществува* $\sigma_0 \in \mathbb{C}$ *такова, че при* $Re(s) > \sigma_0$ *редът е сходящ, а при* $Re(s) < \sigma_0$ *редът е разходящ.*

Доказателство. Ако не е изпълнено нито едно от първите две твърдения в лемата, то полагаме

$$\sigma_0 = \inf\{Re(s) \ : \ \text{редът (324) е сходящ}\ \}.$$

Оставяме на читателя да провери, че при така определеното число σ_0 е изпълнено третото твърдение.

$\square$

Определение 5.20. *Ако за някои* $s \in \mathbb{C}$ *редът* (324) *е сходящ, а за други стойности на* s *— разходящ, то числото* σ_0 *от Лема 5.19* (3) *се нарича абсциса на сходимост на този ред. Ако редът* (324) *е сходящ за всяко* s *считаме, че неговата абсциса на сходимост е* $-\infty$. *Ако пък този ред е разходящ за всяко* s *считаме, че абсцисата му на сходимост е* ∞.

Както е добре известно, с абсолютно сходящи редове се работи значително по-лесно, отколкото с редове, за които знаем само, че са сходящи. Поради това, ако е даден реда на Дирихле (324), естествено е да се заинтересуваме от множеството от стойности на s, за които този ред е абсолютно сходящ. Затова, наред с реда (324) разглеждаме също реда

$$\sum_{n=1}^{\infty} \frac{|a_n|}{n^{\sigma}}. \tag{328}$$

Той също е ред на Дирихле, но на реалната променлива σ. Очевидно е, че

$$\left|\sum_{n=1}^{\infty} \frac{a_n}{n^s}\right| \leq \sum_{n=1}^{\infty} \frac{|a_n|}{n^{\sigma}} \qquad \text{при} \qquad \sigma = Re(s).$$

Тогава, за да определим областта на абсолютна сходимост на (324), е необходимо да определим областта на сходимост на (328). Поради това въвеждаме следното

Определение 5.21. *Абсциса на абсолютна сходимост на реда* (324) *наричаме абсцисата на сходимост на* (328).

В следващата лема е показана връзката между абсцисата на сходимост и абсцисата на абсолютна сходимост на даден ред на Дирихле.

Лема 5.22. *Ако редът* (324) *е сходящ за всяко $s \in \mathbb{C}$, то той е абсолютно сходящ за всяко $s \in \mathbb{C}$. Ако пък този ред има крайна абсциса на сходимост σ_0, то неговата абсциса на абсолютна сходимост σ_a е също крайна и е изпълнено неравенството*

$$0 \leq \sigma_a - \sigma_0 \leq 1. \tag{329}$$

Доказателство. Първо ще отбележим, че ако редът на Дирихле (324) е сходящ в точката $s_1 \in \mathbb{C}$, то той е абсолютно сходящ за всяко $s \in \mathbb{C}$, за което $Re(s - s_1) > 1$. Наистина, нека редът $\sum_{n=1}^{\infty} a_n n^{-s_1}$ е сходящ. Тогава $\lim_{n\to\infty} (a_n n^{-s_1}) = 0$, откъдето следва, че при $\sigma_1 = Re(s_1)$ имаме $\lim_{n\to\infty} (|a_n|\, n^{-\sigma_1}) = 0$. Но тогава, ако положим $Re(s) = \sigma$, имаме

$$\left|\frac{a_n}{n^s}\right| = \frac{|a_n|}{n^{\sigma}} = \frac{|a_n|}{n^{\sigma_1}} \cdot \frac{1}{n^{\sigma-\sigma_1}}. \tag{330}$$

Тъй като $\sigma > \sigma_1 + 1$ редът $\sum_{n=1}^{\infty} n^{-(\sigma-\sigma_1)}$ е сходящ. Оттук и от (330) получаваме, че редът $\sum_{n=1}^{\infty} a_n n^{-s}$ е абсолютно сходящ.

От изложеното разсъждение веднага следва първото твърдение в лемата. Нека сега нашият ред има крайна абсциса на сходимост σ_0. Тогава лявото от неравенствата (329) е очевидно. За да докажем и дясното, нека изберем произволно $\varepsilon > 0$. Тогава редът (324) е сходящ при $s = \sigma_0 + \varepsilon$, откъдето следва, че той е абсолютно сходящ при $s = \sigma_0 + 1 + 2\varepsilon$. Но тогава $\sigma_a \leq \sigma_0 + 1 + 2\varepsilon$ и, тъй като ε може да бъде произволно малко, виждаме, че и дясното от неравенствата (329) е налице.

□

В следващата лема се изяснява връзката между редовете на Дирихле и операцията „конволюция на Дирихле", въведена в Определение 3.23.

Лема 5.23. *Ако редовете на Дирихле*

$$F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}, \qquad G(s) = \sum_{n=1}^{\infty} \frac{g(n)}{n^s} \tag{331}$$

са абсолютно сходящи в точката s, то

$$F(s)G(s) = \sum_{n=1}^{\infty} \frac{h(n)}{n^s}, \tag{332}$$

където $h = f * g$ е конволюцията на Дирихле на аритметичните функции f и g.

Доказателство. От абсолютната сходимост на редовете (331) следва, че

$$F(s)G(s) = \sum_{k,m=1}^{\infty} \frac{f(k)g(m)}{(km)^s} = \sum_{n=1}^{\infty} \sum_{\substack{k,m=1 \\ km=n}}^{\infty} \frac{f(k)g(m)}{(km)^s} = \sum_{n=1}^{\infty} \frac{1}{n^s} \sum_{km=n} f(k)g(m)$$

и, като вземем предвид Определение 3.23, получаваме (332).

□

5.7 Определение и някои основни свойства на $\zeta(s)$

Определение 5.24. *При $Re(s) > 1$ определяме дзета-функцията на Риман $\zeta(s)$ чрез формулата*

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}. \tag{333}$$

Лема 5.25. *Абсцисата на сходимост на реда (333) е равна на 1. Функцията $\zeta(s)$ е аналитична в полуравнината $Re(s) > 1$ и при всяко $k \in \mathbb{N}$ производната от ред k на $\zeta(s)$ се задава чрез*

$$\zeta^{(k)}(s) = \sum_{n=1}^{\infty} \frac{(-\log n)^k}{n^s}. \tag{334}$$

Имаме също

$$|\zeta(s)| \le \frac{\sigma}{\sigma - 1} \qquad \text{при} \qquad Re(s) = \sigma > 1. \tag{335}$$

Доказателство. Първите две твърдения следват непосредствено от Лема 5.18 и Определение 5.24. За да докажем (335) използуваме, че при $Re(s) = \sigma > 1$ са в сила неравенствата

$$|\zeta(s)| \le \sum_{n=1}^{\infty} \frac{1}{|n^s|} = \sum_{n=1}^{\infty} \frac{1}{n^\sigma} \le 1 + \int_1^{\infty} \frac{dt}{t^\sigma} = 1 + \frac{1}{\sigma - 1} = \frac{\sigma}{\sigma - 1}.$$

□

Следва тъждеството на Ойлер за $\zeta(s)$.

Лема 5.26. *Ако $Re(s) > 1$, то е сила тъждеството*

$$\zeta(s) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}, \tag{336}$$

където произведението е по всички прости числа.

Доказателство. Използуваме, че редът (333) е абсолютно сходящ при $Re(s) > 1$ и че функцията $\lambda(n) = n^{-s}$ е напълно мултипликативна. Тогава, като приложим тъждеството на Ойлер (Теорема 3.45), получаваме (336).

$\square$

В теорията на $\zeta(s)$ и в приложенията ѝ е важно да разполагаме с информация за нулите на тази функция. В следващата лема е формулиран най-простия резултат от такъв тип.

Лема 5.27. *Изпълнено е*

$$\zeta(s) \neq 0 \qquad \text{\textit{при}} \qquad Re(s) > 1. \tag{337}$$

Доказателство. Ако $\sigma = Re(s) > 1$ от Лема 5.25 и Лема 5.26 следва

$$\left|\prod_p \left(1 - \frac{1}{p^s}\right)\right| \leq \prod_p \left(1 + \frac{1}{p^\sigma}\right) \leq \prod_p \left(1 + \frac{1}{p^\sigma} + \frac{1}{p^{2\sigma}} + \dots\right) = \zeta(\sigma) \leq \frac{\sigma}{\sigma - 1}.$$

Тогава

$$1 = \left|\zeta(s) \prod_p \left(1 - \frac{1}{p^s}\right)\right| \leq |\zeta(s)| \frac{\sigma}{\sigma - 1},$$

откъдето

$$|\zeta(s)| \geq \frac{\sigma - 1}{\sigma}.$$

$\square$

От следващата лема се убеждаваме, че редове на Дирихле, коефициентите на които се задават чрез въведените досега аритметични функции, се изразяват чрез дзета-функцията на Риман. Известни са много такива тъждества, но тук ще се задоволим само с три от тях.

Лема 5.28. *При $Re(s) > 1$ са в сила тъждествата*

$$\zeta(s)^{-1} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}, \tag{338}$$

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}, \tag{339}$$

$$\zeta^2(s) = \sum_{n=1}^{\infty} \frac{\tau(n)}{n^s}. \tag{340}$$

Доказателство. За да докажем (338), умножаваме редовете

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \qquad \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}$$

по правилото от Лема 5.23 и използуваме Лема 3.34. Аналогично, като умножим редовете

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \qquad \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}$$

и вземем предвид Лема 3.42, получаваме (339). По същия начин се убеждаваме и във верността на (340).

$\square$

Лема 5.29. *Функцията $\zeta(s)$ притежава мероморфно продължение в полуравнината $Re(s) > 0$, като там има полюс само в точката $s = 1$. Този полюс е прост и е с резудуум 1. Освен това, за всяко $M \in \mathbb{N}$ при $Re(s) > 0$ е в сила равенството*

$$\zeta(s) = \sum_{n=1}^{M} \frac{1}{n^s} + \frac{M^{1-s}}{s-1} - \frac{1}{2M^s} + s \int_{M}^{\infty} \frac{\rho(t)}{t^{s+1}}\, dt, \tag{341}$$

където $\rho(t)$ е функцията от Определение 2.2.

Доказателство. Ако $M, N \in \mathbb{N}$, $M < N$, то като приложим първата сумационна формула на Ойлер (Лема 2.4) получаваме

$$\sum_{M<n\leq N} n^{-s} = \int_{M}^{N} t^{-s}\, dt + \rho(N)N^{-s} - \rho(M)M^{-s} - \int_{M}^{N} \rho(t)\, \frac{d}{dt}\left(t^{-s}\right)\, dt$$

$$= \frac{M^{1-s}}{s-1} - \frac{N^{1-s}}{s-1} + \frac{1}{2N^s} - \frac{1}{2M^s} + s \int_{M}^{N} \frac{\rho(t)}{t^{s+1}}\, dt.$$

Нека $Re(s) > 1$. Извършваме в последното равенство граничен преход $N \to \infty$ и получаваме

$$\zeta(s) - \sum_{n=1}^{M} n^{-s} = \sum_{n>M} n^{-s} = \frac{M^{1-s}}{s-1} - \frac{1}{2M^s} + s \int_{M}^{\infty} \frac{\rho(t)}{t^{s+1}}\, dt,$$

с което се убеждаваме, че (341) е вярно при $Re(s) > 1$. Като положим $M = 1$ в равенството (341) виждаме, че при $Re(s) > 1$ е изпълнено

$$\zeta(s) = \frac{1}{s-1} + \frac{1}{2} + s \int_{1}^{\infty} \frac{\rho(t)}{t^{s+1}}\, dt. \tag{342}$$

Но за произволно $\sigma' > 0$ интегралът $\int_1^\infty \frac{\rho(t)}{t^{s+1}}\, dt$ е равномерно сходящ в множеството $Re(s) \geq \sigma'$ и подинтегралната му функция е аналитична по отношение на s. Поради това този интеграл е аналитична функция при $Re(s) > 0$. Следователно равенството

(342) задава продължение на $\zeta(s)$ до мероморфна функция в $Re(s) > 0$, която има прост полюс с резудуум 1 в точката $s = 1$.

Накрая, тъй като (341) е вярно за $Re(s) > 1$, то по принципа за аналитично продължение следва верността на това равенство и при $Re(s) > 0$.

$\square$

Както ще видим по-нататък, важно е да оценим $\zeta(s)$ и $\zeta'(s)$ върху и вдясно от правата $Re(s) = 1$. Резултат от такъв тип е изложен в следващата лема.

Лема 5.30. *В множеството*

$$1 \le \sigma \le 2, \qquad |\tau| \ge 3 \tag{343}$$

са в сила оценките

$$|\zeta(\sigma + i\tau)| \le 10 \log |\tau|, \tag{344}$$

$$|\zeta'(\sigma + i\tau)| \le 10 \log^2 |\tau|. \tag{345}$$

Доказателство. Тъй като $|\zeta(s)| = |\zeta(\overline{s})|$ и $|\zeta'(s)| = |\zeta'(\overline{s})|$, то е достатъчно да докажем (344) и (345) при

$$1 \le \sigma \le 2, \qquad \tau \ge 3. \tag{346}$$

И така, нека $s = \sigma + i\tau$ и нека е изпълнено (346). Използуваме тъждеството (341) от Лема 5.29 при $M = [\tau]$ и при $s = \sigma + i\tau$. Лесно се проверява, че ако са налице условията (346), то имаме

$$|s - 1| \ge 1, \qquad |s| \le 2\tau. \tag{347}$$

Тогава от (347), неравенството на триъгълника, Лема 2.3 (2) и Лема 5.29 следва

$$\begin{aligned}
|\zeta(s)| &\le \sum_{n=1}^{[\tau]} \frac{1}{n^\sigma} + \frac{[\tau]^{1-\sigma}}{|s-1|} + \frac{1}{2} + |s| \int_{[\tau]}^{\infty} \frac{|\rho(t)|}{t^{\sigma+1}}\, dt \\
&\le \sum_{n=1}^{[\tau]} \frac{1}{n} + 2 + \tau \int_{[\tau]}^{\infty} \frac{dt}{t^2} \\
&\le \log \tau + 3 + \frac{\tau}{[\tau]} \\
&\le \log \tau + 5.
\end{aligned}$$

С това неравенството (344) е доказано.

Сега ще докажем и (345). Нека $s=\sigma+i\tau$, като е изпълнено (346). Диференцираме равенството (341) от Лема 5.29, след което прилагаме неравенството на триъгълника, Лема 2.3 (2) и (347). Получаваме

$$|\zeta'(s)| = \left| -\sum_{n=1}^{M} \frac{\log n}{n^s} - \frac{M^{1-s}}{s-1}\log M - \frac{M^{1-s}}{(s-1)^2} + \frac{\log M}{2M^s} + \int_M^\infty \frac{\rho(t)}{t^{s+1}}\,dt + s\,\frac{d}{ds}\int_M^\infty \frac{\rho(t)}{t^{s+1}}\,dt \right|$$

$$\le \sum_{n=1}^{M} \frac{\log n}{n} + \frac{\log M}{|s-1|} + \frac{1}{|s-1|^2} + \frac{\log M}{2M} + \frac{1}{2}\int_M^\infty \frac{dt}{t^2} + 2\tau \left| \frac{d}{ds}\int_M^\infty \frac{\rho(t)}{t^{s+1}}\,dt \right|$$

$$\le \log^2 M + \log M + 2 + 2\tau \left| \frac{d}{ds}\int_M^\infty \frac{\rho(t)}{t^{s+1}}\,dt \right|. \tag{348}$$

Остана да оценим последното събираемо в горния израз. За целта внасяме диференцирането под знака на интеграла, т.е. използуваме равенството

$$\frac{d}{ds}\int_M^\infty \frac{\rho(t)}{t^{s+1}}\,dt = -\int_M^\infty \frac{\rho(t)\,\log t}{t^{s+1}}\,dt. \tag{349}$$

Тази операция е законна, тъй като и двата интеграла в горната формула са равномерно сходящи във всяко компактно подмножество на полуравнината $Re(s)>0$, а подинтегралните функции са аналитични по отношение на s.

Тогава от (348), (349) и Лема 2.3 (2) следва

$$|\zeta'(s)| \le \log^2 M + \log M + 2 + \tau\int_M^\infty \frac{\log t}{t^2}\,dt.$$

Избираме $M=[\tau]$ и, като вземем предвид, че

$$\int_M^\infty \frac{\log t}{t^2}\,dt = -\int_M^\infty \log t\; d\left(\frac{1}{t}\right) = \frac{\log M}{M} + \int_M^\infty \frac{dt}{t^2} = \frac{\log M+1}{M},$$

получаваме

$$|\zeta'(s)| \le \log^2\tau + \log\tau + 2 + \frac{\tau(\log\tau+1)}{[\tau]} \le 10\,\log^2\tau.$$

С това лемата е доказана.

□

Лема 5.31. *При $\sigma>1$ и при всяко $\tau\in\mathbb{R}$ е изпълнено*

$$\left|\zeta^3(\sigma)\zeta^4(\sigma+i\tau)\zeta(\sigma+2i\tau)\right| \ge 1. \tag{350}$$

Доказателство. Първо ще установим, че

$$\left|(1-r)^3(1-re^{i\varphi})^4(1-re^{2i\varphi})\right|^{-1} \geq 1 \qquad \text{при} \qquad 0<r<1, \quad \varphi\in\mathbb{R}. \tag{351}$$

За тази цел разглеждаме израза

$$\mathcal{J} = \log\left|(1-r)^3(1-re^{i\varphi})^4(1-re^{2i\varphi})\right|^{-1}. \tag{352}$$

Ясно е, че

$$\mathcal{J} = -3\log(1-r) - 4\log\left|1-re^{i\varphi}\right| - \log\left|1-re^{2i\varphi}\right|.$$

Използуваме познатото разлагане в степенен ред

$$-\log(1-w) = \sum_{n=1}^{\infty}\frac{w^n}{n} \qquad \text{при} \qquad w\in\mathbb{C}, \quad |w|<1$$

и вземаме предвид равенството $Re(\log w) = \log|w|$. Получаваме

$$\begin{aligned}
\mathcal{J} &= Re\Big(-3\log(1-r) - 4\log\left(1-re^{i\varphi}\right) - \log\left(1-re^{2i\varphi}\right)\Big) \\
&= Re\left(3\sum_{n=1}^{\infty}\frac{r^n}{n} + 4\sum_{n=1}^{\infty}\frac{r^n e^{in\varphi}}{n} + \sum_{n=1}^{\infty}\frac{r^n e^{2in\varphi}}{n}\right) \\
&= 3\sum_{n=1}^{\infty}\frac{r^n}{n} + 4\sum_{n=1}^{\infty}\frac{r^n Re\left(e^{in\varphi}\right)}{n} + \sum_{n=1}^{\infty}\frac{r^n Re\left(e^{2in\varphi}\right)}{n} \\
&= 3\sum_{n=1}^{\infty}\frac{r^n}{n} + 4\sum_{n=1}^{\infty}\frac{r^n\cos(n\varphi)}{n} + \sum_{n=1}^{\infty}\frac{r^n\cos(2n\varphi)}{n} \\
&= \sum_{n=1}^{\infty}\frac{r^n}{n}\big(3+4\cos(n\varphi)+\cos(2n\varphi)\big).
\end{aligned}$$

Но за всяко $\alpha\in\mathbb{R}$ имаме

$$3+4\cos\alpha+\cos 2\alpha = 2\left(1+2\cos\alpha+\cos^2\alpha\right) = 2\left(1+\cos\alpha\right)^2 \geq 0.$$

Тогава имаме $\mathcal{J}\geq 0$ и, като използуваме (352), получаваме неравенството (351).

За да докажем (350), използуваме Лема 5.26 и получаваме

$$\begin{aligned}
\left|\zeta^3(\sigma)\zeta^4(\sigma+i\tau)\zeta(\sigma+2i\tau)\right| &= \left|\prod_p\left(1-\frac{1}{p^\sigma}\right)^{-3}\left(1-\frac{1}{p^{\sigma+i\tau}}\right)^{-4}\left(1-\frac{1}{p^{\sigma+2i\tau}}\right)^{-1}\right| \\
&= \prod_p\left|\left(1-\frac{1}{p^\sigma}\right)^{3}\left(1-\frac{e^{-i\tau\log p}}{p^\sigma}\right)^{4}\left(1-\frac{e^{-2i\tau\log p}}{p^\sigma}\right)\right|^{-1}.
\end{aligned}$$

За всеки от множителите в горното произведение прилагаме неравенството (351) с параметри $r = p^{-\sigma}$ и $\varphi = -\tau \log p$ и получаваме (350).

$\square$

Следва важен резултат за нулите на $\zeta(s)$, който стои в основата на доказателството на асимптотичния закон за разпределение на простите числа.

Теорема 5.32. *За всяко $\tau \in \mathbb{R}$ е изпълнено $\zeta(1 + i\tau) \neq 0$.*

Доказателство. Функцията $\zeta(s)$ притежава полюс в точката $s = 1$, следователно не може да се анулира в нея. Да допуснем, че за някое $\tau_0 \in \mathbb{R}$, $\tau_0 \neq 0$ е изпълнено

$$\zeta(1 + i\tau_0) = 0.$$

От Лема 5.31 следва, че

$$1 \leq \left|\zeta^3(\sigma)\zeta^4(\sigma + i\tau_0)\zeta(\sigma + 2i\tau_0)\right| \qquad \text{при} \quad \sigma > 1. \tag{353}$$

Нека точката $s_0 = 1 + i\tau_0$ е k-кратна нула на $\zeta(s)$, като $k \in \mathbb{N}$. Тогава в околност на s_0 имаме

$$|\zeta(s)| \ll_{\tau_0} |s - s_0|^k,$$

откъдето

$$|\zeta(\sigma + i\tau_0)| \ll_{\tau_0} (\sigma - 1)^k \qquad \text{при} \quad 1 < \sigma < \eta, \quad \text{където} \quad \eta = \eta(\tau_0) > 1. \tag{354}$$

По-нататък, според Лема 5.25 имаме

$$\zeta(\sigma) \leq \frac{2}{\sigma - 1} \qquad \text{при} \quad 1 < \sigma \leq 2. \tag{355}$$

Накрая, тъй като $\tau_0 \neq 0$, то от Лема 5.29 виждаме, че $\zeta(s)$ е аналитична и, следователно, ограничена в околност на точката $1 + 2i\tau_0$. Тогава имаме

$$|\zeta(\sigma + 2i\tau_0)| \ll_{\tau_0} 1 \qquad \text{при} \quad 1 < \sigma < \eta', \quad \text{където} \quad \eta' = \eta'(\tau_0) > 1. \tag{356}$$

От (353) – (356) следва

$$1 \ll_{\tau_0} (\sigma - 1)^{4k-3} \qquad \text{при} \quad 1 < \sigma < \eta'', \quad \text{където} \quad \eta'' = \eta''(\tau_0) > 1.$$

Но $4k - 3 \geq 1$, следователно ако $\sigma \to 1$, като $\sigma > 1$, получаваме противоречие. С това теоремата е доказана.

$\square$

Лема 5.33. *В множеството*

$$\sigma \geq 1, \qquad |\tau| \geq 3 \tag{357}$$

е в сила оценката

$$\frac{\zeta'(\sigma + i\tau)}{\zeta(\sigma + i\tau)} \ll \log^9 |\tau|, \tag{358}$$

като константата в знака $\ll$ е абсолютна.

Доказателство. Можем да считаме, че $1 \le \sigma \le 2$, тъй като при $\sigma > 2$ изразът в лявата страна на (358) е равен на $O(1)$. По-нататък, от съображенията, изложени в началото на доказателството на Лема 5.30, следва че е достатъчно е да докажем (358) при

$$1 \le \sigma \le 2, \qquad \tau \ge 3. \tag{359}$$

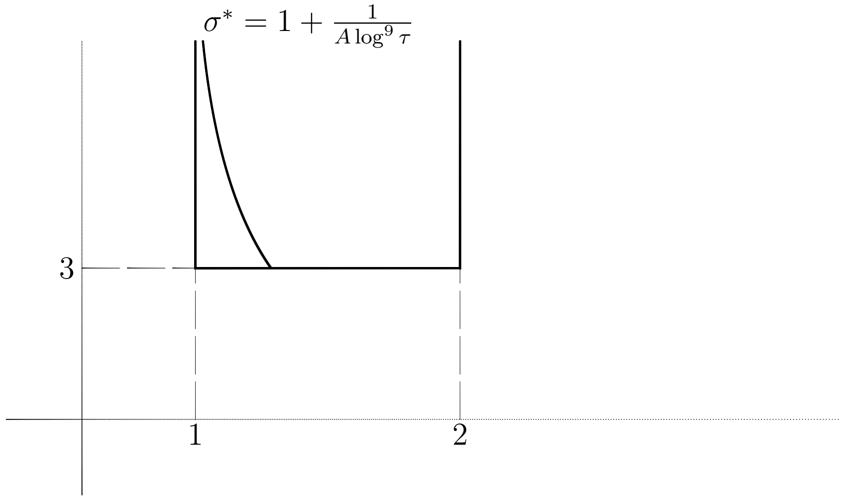
Означаваме

$$\sigma^* = \sigma^*(\tau) = 1 + \frac{1}{A \log^9 \tau}\,, \tag{360}$$

където $A > 10$ е константа, която ще изберем по-късно. Разглеждаме множеството от точки $s = \sigma + i\tau$ за които е изпълнено

$$\sigma^* \le \sigma \le 2, \qquad \tau \ge 3. \tag{361}$$

Контурът на това множество може да се види на следния чертеж.



Нека оценим функцията $|\zeta'(s)/\zeta(s)|$ когато $s = \sigma + i\tau$ принадлежи на множеството (361). За тази цел първо оценяваме отдолу $|\zeta(s)|$. Прилагаме Лема 5.31 и получаваме

$$|\zeta(\sigma + i\tau)| \ge |\zeta(\sigma)|^{-\frac{3}{4}}\, |\zeta(\sigma + 2i\tau)|^{-\frac{1}{4}}. \tag{362}$$

От неравенството (335) в Лема 5.25, от (360) и (361) следва

$$\zeta(\sigma)^{-\frac{3}{4}} \ge \left(\frac{\sigma - 1}{2}\right)^{\frac{3}{4}} \ge \left(\frac{\sigma^* - 1}{2}\right)^{\frac{3}{4}} = \left(2A \log^9 \tau\right)^{-\frac{3}{4}}.$$

По-нататък, като използуваме неравенството (344) от Лема 5.30 намираме, че

$$|\zeta(\sigma + 2i\tau)|^{-\frac{1}{4}} \ge \left(10\, \log(2\tau)\right)^{-\frac{1}{4}} \ge (\,20\, \log \tau\,)^{-\frac{1}{4}}.$$

От горните две неравенства и от (362) виждаме, че в множеството (361) имаме

$$|\zeta(\sigma+i\tau)| \geq \left(2A\log^9\tau\right)^{-\frac{3}{4}} \left(\,20\,\log\tau\,\right)^{-\frac{1}{4}} \geq \left(5\,A^{\frac{3}{4}}\,\log^7\tau\right)^{-1}. \tag{363}$$

Сега ще оценим отдолу $|\zeta(s)|$, когато $s=\sigma+i\tau$ принадлежи на множеството

$$1\leq\sigma\leq\sigma^*, \qquad \tau\geq 3. \tag{364}$$

За тази цел първо използуваме, че

$$|\zeta(\sigma^*+i\tau)-\zeta(\sigma+i\tau)| = \left|\int\limits_{\sigma}^{\sigma^*}\zeta'(u+i\tau)\,du\right| \leq (\sigma^*-\sigma)\max_{1\leq u\leq\sigma^*}|\zeta'(u+i\tau)|\,,$$

след което прилагаме (360), (364) и оценката (345) от Лема 5.30. Получаваме

$$|\zeta(\sigma^*+i\tau)-\zeta(\sigma+i\tau)| \leq \frac{10}{A\,\log^7\tau}.$$

Тогава, като приложим неравенството на триъгълника, намираме, че

$$|\zeta(\sigma+i\tau)| \geq |\zeta(\sigma^*+i\tau)| - |\zeta(\sigma^*+i\tau)-\zeta(\sigma+i\tau)| \geq |\zeta(\sigma^*+i\tau)| - \frac{10}{A\,\log^7\tau}.$$

Оттук и от факта, че оценката (363) е вярна при $\sigma=\sigma^*$, виждаме, че в множеството, определено от (364), имаме

$$|\zeta(\sigma+i\tau)| \geq \left(\frac{1}{5A^{\frac{3}{4}}}-\frac{10}{A}\right)(\log\tau)^{-7}.$$

Сега определяме A така, че

$$\frac{1}{5A^{\frac{3}{4}}} \geq \frac{20}{A}$$

или, все едно, $A\geq 10^8$. Тогава, ако изберем например $A=10^8$, то както в множеството (361), така и в множеството (364) е изпълнено

$$|\zeta(\sigma+i\tau)| \geq 10^{-7}\,(\log\tau)^{-7}. \tag{365}$$

Следователно последното неравенство е изпълнено в множеството, определено от (359).

Остава да използуваме оценката за $\zeta'(s)$, приведена във формула (345) от Лема 5.30. От нея и от (365) следва, че в множеството (359) е изпълнено

$$\left|\frac{\zeta'(\sigma+i\tau)}{\zeta(\sigma+i\tau)}\right| \leq 10^8\log^9\tau.$$

С това лемата е доказана.

$\square$

5.8 Асимптотичен закон за разпределение на простите числа

В настоящия параграф ще използваме свойствата на дзета-функцията на Риман, за да докажем Асимптотичния закон за разпределение на простите числа:

Теорема 5.34 (Адамар, Вале-Пусен)**.** *За функцията $\pi(x)$ е в сила асимптотичната формула*

$$\pi(x) \sim \frac{x}{\log x} \qquad \textit{при} \qquad x \to \infty. \tag{366}$$

За да докажем тази знаменита теорема първо ще формулираме и докажем две леми, в които се установява, че формулата (366) е еквивалентна на други асимптотични формули.

Лема 5.35. *Следните три твърдения са еквивалентни:*

$$\pi(x) \sim \frac{x}{\log x} \qquad \textit{при} \qquad x \to \infty, \tag{367}$$

$$\psi(x) \sim x \qquad \textit{при} \qquad x \to \infty, \tag{368}$$

$$\theta(x) \sim x \qquad \textit{при} \qquad x \to \infty. \tag{369}$$

Доказателство. Еквивалентността на (368) и (369) следва непосредствено от Лема 5.5. Еквивалентността на (367) и (369) може да се докаже, като се разсъждава както при доказателството на Лема 5.6. Друг възможен подход е да се използва преобразованието на Абел (Лема 2.1), за да се установи формулата

$$\theta(x) = \pi(x)\log x - \int\limits_2^x \frac{\pi(t)}{t}\,dt.$$

Последният интеграл може да се оцени, като се използва Теоремата на Чебишев (Теорема 5.4) и тогава се получава

$$\theta(x) = \pi(x)\log x + O\left(\frac{x}{\log x}\right).$$

Подробностите оставяме на читателя.

□

Тясно свързана с функцията на Чебишев $\psi(x)$ е функцията $\Phi(x)$, определена чрез

$$\Phi(x) = \int\limits_2^x \psi(t)\,dt. \tag{370}$$

Оказва се, че изследването на асимптотиката на $\Phi(x)$ при $x \to \infty$ е по-лесно от това на $\psi(x)$, тъй като всички несобствени интеграли, които възникват в процеса на работа, са абсолютно сходящи. От друга страна, както ще видим от следващата лема, за да докажем асимптотичния закон за разпределение на простите числа е достатъчно да установим асимптотична формула за $\Phi(x)$. Тези факти оправдават въвеждането и изучаването на горната функция.

Лема 5.36. *Следните две твърдения са еквивалентни:*

$$\psi(x) \sim x \qquad \text{при} \qquad x \to \infty, \tag{371}$$

$$\Phi(x) \sim \frac{1}{2}x^2 \qquad \text{при} \qquad x \to \infty. \tag{372}$$

Доказателство. Лесно се установява, че ако е изпълнено (371), то следва (372) (проверката предоставяме на читателя).

Нека сега допуснем, че е вярно (372). Тъй като функцията $\psi(x)$ е монотонно растяща, имаме

$$\psi(x_1) \le \frac{\Phi(x_2) - \Phi(x_1)}{x_2 - x_1} \le \psi(x_2) \qquad \text{при} \qquad 2 \le x_1 < x_2. \tag{373}$$

Избираме произволно $\varepsilon \in \big(0, \frac{1}{100}\big)$ и нека $\delta \in (0, \frac{1}{2})$ е параметър, който ще изберем по-късно в зависимост от ε. Тъй като е вярно (372), то съществува $x_0 = x_0(\varepsilon) \ge 2$ такова, че

$$(1-\varepsilon)\frac{1}{2}x^2 \le \Phi(x) \le (1+\varepsilon)\frac{1}{2}x^2 \qquad \text{при} \qquad x \ge x_0. \tag{374}$$

Прилагаме лявото от неравенствата (373) за

$$x_1 = x, \qquad x_2 = (1+\delta)x$$

и получаваме, че при $x \ge x_0$ е изпълнено

$$\frac{\psi(x)}{x} \le \frac{\Phi\big((1+\delta)(x)\big) - \Phi(x)}{\delta x^2} \le \frac{(1+\varepsilon)\,\frac{1}{2}\,(1+\delta)^2\,x^2 - (1-\varepsilon)\,\frac{1}{2}\,x^2}{\delta x^2}$$

$$= \frac{(1+\varepsilon)(1+\delta)^2 - (1-\varepsilon)}{2\delta} \le \frac{2\delta + \delta^2 + 5\varepsilon}{2\delta} \le 1 + \delta + 5\varepsilon\delta^{-1}.$$

Избираме $\delta = \sqrt{\varepsilon}$ и получаваме, че при $x \ge x_0$ е вярно неравенството

$$\frac{\psi(x)}{x} \le 1 + 6\sqrt{\varepsilon},$$

следователно

$$\limsup_{x\to\infty} \frac{\psi(x)}{x} \le 1 + 6\sqrt{\varepsilon}.$$

Тъй като ε може да бъде произволно малко, виждаме, че

$$\limsup_{x\to\infty} \frac{\psi(x)}{x} \le 1. \tag{375}$$

Сега прилагаме дясното от неравенствата (373) за

$$x_1 = (1-\delta)x, \qquad x_2 = x$$

и, като вземем предвид (374), получаваме, че при $x \geq 2x_0$ е изпълнено

$$\frac{\psi(x)}{x} \geq \frac{\Phi(x) - \Phi\big((1-\delta)x\big)}{\delta x^2} \geq \frac{(1-\varepsilon)\,\frac{1}{2}\,x^2 - (1+\varepsilon)\,\frac{1}{2}\,(1-\delta)^2\,x^2}{\delta x^2}$$

$$= \frac{(1-\varepsilon) - (1+\varepsilon)(1-\delta)^2}{2\delta} \geq \frac{2\delta - \delta^2 - 5\varepsilon}{2\delta} \geq 1 - \delta - 5\varepsilon\delta^{-1}.$$

Като положим $\delta = \sqrt{\varepsilon}$ виждаме, че

$$\liminf_{x\to\infty} \frac{\psi(x)}{x} \geq 1 - 6\sqrt{\varepsilon}.$$

Но $\varepsilon > 0$ може да бъде произволно малко, следователно

$$\liminf_{x\to\infty} \frac{\psi(x)}{x} \geq 1.$$

От последната формула и от (375) следва (371).

□

Както ще видим по-нататък, при изследването на $\Phi(x)$ се появява функцията

$$f(x) = \begin{cases} 1-x & \text{при} \quad 0 < x < 1, \\ 0 & \text{при} \quad x \geq 1. \end{cases} \tag{376}$$

В следващата лема е дадено нейно интегрално представяне.

Лема 5.37. *При произволно $c > 0$ за функцията, определена чрез* (376), *е в сила тъждеството*

$$f(x) = \frac{1}{2\pi i} \int\limits_{c-i\infty}^{c+i\infty} \frac{x^{-s}}{s(s+1)}\, ds. \tag{377}$$

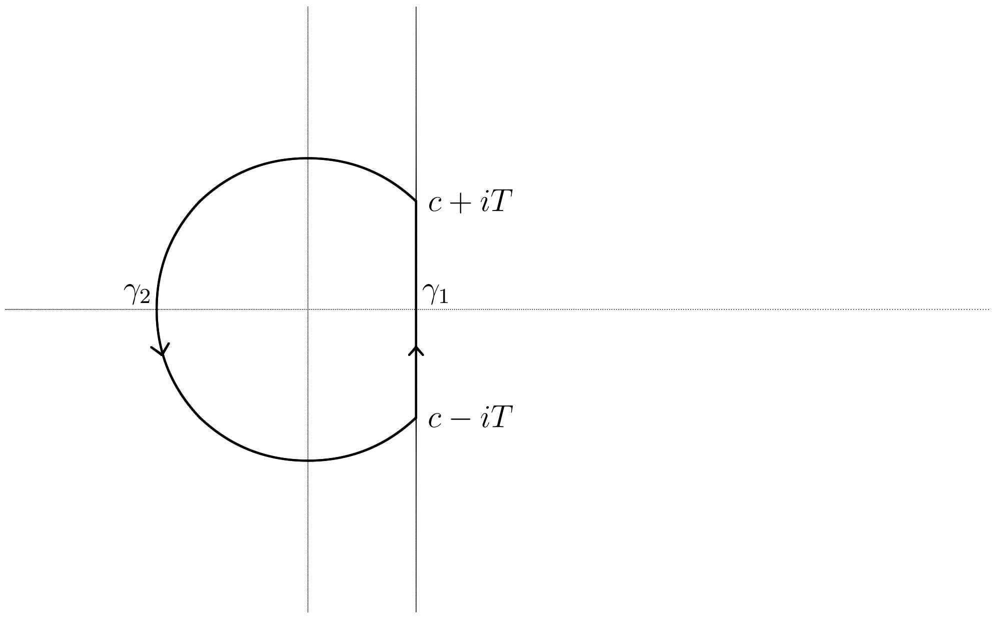
Доказателство. Нека $T \geq 10$ е параметър нека означим

$$F(s) = \frac{x^{-s}}{s(s+1)}. \tag{378}$$

Да отбележим, че интегралът в дясната страна на равенството (377) е абсолютно сходящ, тъй като

$$\max_{Re(s)=c} |F(s)| = \frac{x^{-c}}{|s(s+1)|} \ll_c x^{-c}\,(1 + |Im(s)|)^{-2}\,.$$

Първо разглеждаме случая $0 < x < 1$. Означаваме с γ_1 е отсечката с начало $c - iT$ и край $c + iT$ и нека γ_2 е дъгата от окръжност с център точката $s = 0$ и радиус $\sqrt{c^2+T^2}$, която започва от точката $c + iT$, пресича реалната ос в отрицателно число и завършва в точката $c - iT$. Да означим с γ контура, който се състои от отсечката γ_1 и от дъгата γ_2. Контурът γ е даден на следния чертеж.



Функцията $F(s)$ притежава прости полюси в точките $s = 0$ и $s = -1$. Очевидно тези точки са вътре в контура γ и, тъй като $\mathrm{Res}_{s=0}F(s) = 1$, $\mathrm{Res}_{s=-1}F(s) = -x$, то от теоремата за резидуумите следва

$$\int_{\gamma} F(s)\,ds = 2\pi i(1-x). \tag{379}$$

От друга страна имаме

$$\int_{\gamma} F(s)\,ds = I_1 + I_2, \qquad I_k = \int_{\gamma_k} F(s)\,ds, \qquad k = 1, 2. \tag{380}$$

От определението на γ_1 веднага следва

$$\lim_{T\to\infty} I_1 = \int_{c-i\infty}^{c+i\infty} F(s)\,ds. \tag{381}$$

Да разгледаме I_2. Ясно е, че

$$|I_2| \le l(\gamma_2) \max_{s\in\gamma_2} |F(s)|, \tag{382}$$

където $l(\gamma_2)$ е дължината на дъгата γ_2. Очевидно

$$l(\gamma_2) \le 2\pi\sqrt{c^2 + T^2}. \tag{383}$$

По-нататък, когато $s \in \gamma_2$ имаме

$$|x^{-s}| = x^{-Re(s)} \le x^{-c}$$

и също така

$$|s(s+1)| \geq |s|(|s|-1) \geq \frac{|s|^2}{2} = \frac{c^2+T^2}{2},$$

следователно

$$\max_{s\in\gamma_2} |F(s)| \leq \frac{2x^{-c}}{c^2+T^2}. \tag{384}$$

От (382) – (384) получаваме

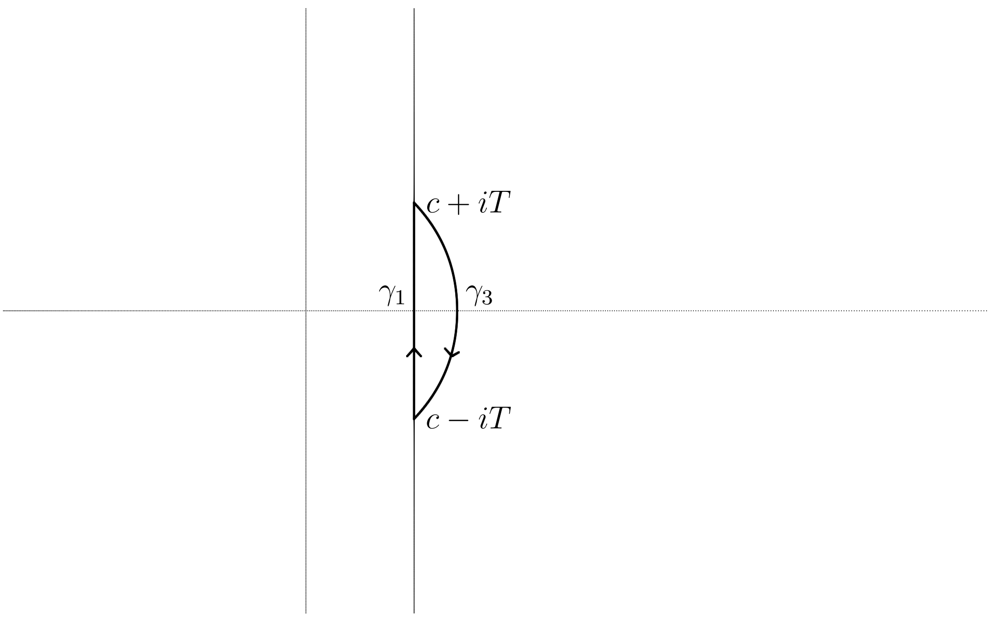
$$|I_2| \leq \frac{4\pi x^{-c}}{\sqrt{c^2+T^2}},$$

откъдето

$$\lim_{T\to\infty} I_2 = 0. \tag{385}$$

Тогава в случая $0 < x < 1$ равенството (377) следва от (378) – (381) и (385).

Ако $x \geq 1$ разсъжденията са аналогични, но вместо по контура γ интегрираме функцията $F(s)$ по γ^*. Контурът γ^* е съставен от отсечката γ_1 и от кривата γ_3, която е дъга от окръжност с център точката $s = 0$ и радиус $\sqrt{c^2+T^2}$, започваща от точката $c+iT$, пресичаща реалната ос в положително число и свършваща в точката $c-iT$. Контурът γ^* е даден на следния чертеж.



Тъй като $F(s)$ е аналитична вътре и по контура γ^*, то от теоремата на Коши следва

$$\int\limits_{\gamma^*} F(s)\,ds = 0.$$

Като използваме това равенство и извършим пресмятания, подобни на предишните, получаваме че (377) е вярно и в случая $x \geq 1$. Изчисленията предоставяме на читателя.

$\square$

В следващата лема е дадена интегрално представяне за $\Phi(x)$, като в подинтегралната функция участва логаритмичната производна на $\zeta(s)$.

Лема 5.38. *При произволно $x \geq 2$ за функцията $\Phi(x)$, определена чрез* (370) *е изпълнено*

$$\Phi(x) = \frac{1}{2\pi i} \int\limits_{2-i\infty}^{2+i\infty} \left(-\frac{\zeta'(s)}{\zeta(s)} \right) \frac{x^{1+s}}{s(s+1)}\, ds. \tag{386}$$

Доказателство. Ще приложим Лема 5.37. От (285), (370) и (376) следва

$$\Phi(x) = \int\limits_2^x \sum_{n \leq t} \Lambda(n)\, dt = \sum_{n \leq x} \Lambda(n) \int\limits_n^x dt = \sum_{n \leq x} \Lambda(n)(x-n) = x \sum_{n=1}^{\infty} \Lambda(n) f\left(\frac{n}{x}\right).$$

Използуваме тъждеството (377) при $c = 2$ и получаваме

$$\Phi(x) = x \sum_{n=1}^{\infty} \Lambda(n)\, \frac{1}{2\pi i} \int\limits_{2-i\infty}^{2+i\infty} \frac{x^s}{n^s\, s(s+1)}\, ds.$$

Сега сменяме реда на сумиране и интегриране. Тази операция е законна, тъй като при $s = 2 + i\tau$ имаме

$$\left| \frac{\Lambda(n)\, x^s}{n^s\, s(s+1)} \right| \leq \frac{\Lambda(n)\, x^2}{n^2\, (4+\tau^2)}$$

и понеже редът $\sum_{n=1}^{\infty} \Lambda(n)\, n^{-2}$ и интегралът $\int_{-\infty}^{\infty} (4+\tau^2)^{-1}\, d\tau$ са сходящи. Тогава

$$\Phi(x) = \frac{1}{2\pi i} \int\limits_{2-i\infty}^{2+i\infty} \left(\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s} \right) \frac{x^{1+s}}{s(s+1)}\, ds$$

и, като се възползуваме от тъждеството (339) на Лема 5.28, получаваме (386).

$\square$

Следва доказателството на асимптотичния закон за разпределението на простите числа.

Доказателство на Теорема 5.34. От Лема 5.35 и Лема 5.36 следва, че за да докажем асимптотичния закон за разпределението на простите числа е достатъчно да установим, че

$$\Phi(x) \sim \frac{x^2}{2} \qquad \text{при} \qquad x \to \infty. \tag{387}$$

Да положим

$$\Xi(s) = \Xi(s;x) = -\frac{\zeta'(s)}{\zeta(s)} \frac{x^{1+s}}{s(s+1)} \tag{388}$$

В Лема 5.38 установихме равенството

$$\Phi(x) = \frac{1}{2\pi i} \int\limits_{2-i\infty}^{2+i\infty} \Xi(s)\, ds. \tag{389}$$

Избираме $\varepsilon > 0$. Нашата цел е да докажем, че ако

$$R(x) = \Phi(x) - \frac{x^2}{2}, \tag{390}$$

то съществува $x_0 = x_0(\varepsilon)$ такова, че

$$|R(x)| \le \varepsilon x^2 \qquad \text{при} \qquad x \ge x_0. \tag{391}$$

Нека T и T_0 са параметри, които ще изберем по-късно. Засега предполагаме, че

$$3 \le T_0 < T. \tag{392}$$

Според Теорема 5.32 имаме $\zeta(1 + i\tau) \ne 0$ при $|\tau| \le T_0$. Тогава $\zeta(s) \ne 0$ в околност на всяка точка от отсечката Γ_0 с краища $1 - iT_0$ и $1 + iT_0$ (за които считаме, че принадлежат на Γ_0). Следователно за всяка точка $s_0 \in \Gamma_0$ съществува отворено кръгче $\mathcal{U}(s_0)$ с център s_0 такова, че $\zeta(s) \ne 0$ при $s \in \mathcal{U}(s_0)$. Но отсечката Γ_0 е компактно множество и затова се покрива само от краен брой от посочените кръгчета. Оттук следва, че съществува $\eta = \eta(T_0)$ удовлетворяващо

$$\frac{1}{2} < \eta < 1 \tag{393}$$

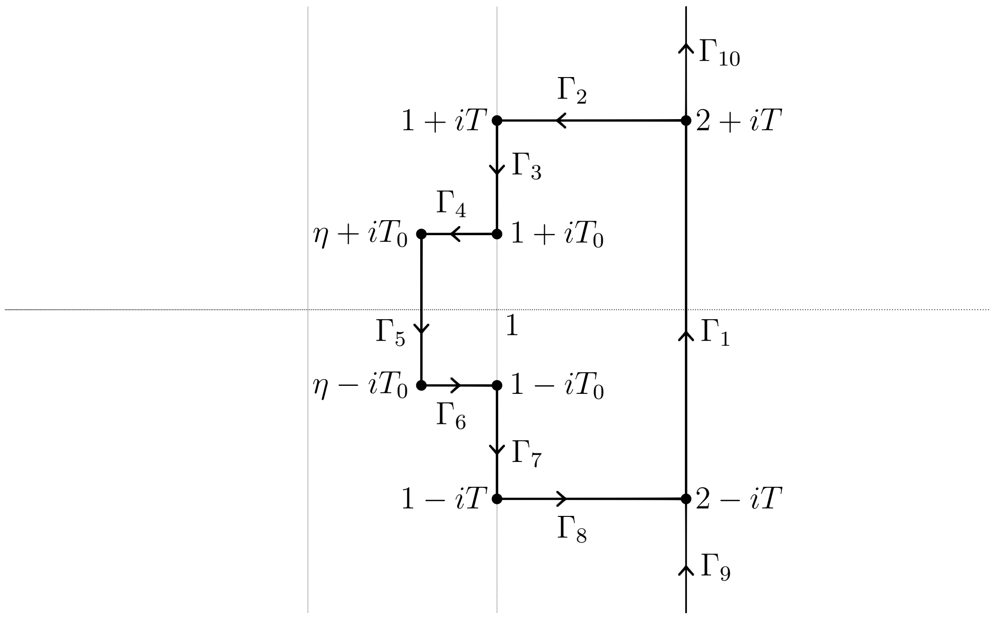
и такова, че

$$\zeta(\sigma + i\tau) \ne 0 \qquad \text{при} \qquad \eta \le \sigma \le 1, \qquad |\tau| \le T_0. \tag{394}$$

Интегрираме функцията $\Xi(s)$ върху затворения контур Γ, който се състои от:

- отсечката Γ_1 с начало точката $2 - iT$ и край $2 + iT$,
- отсечката Γ_2 с начало точката $2 + iT$ и край $1 + iT$,
- отсечката Γ_3 с начало точката $1 + iT$ и край $1 + iT_0$,
- отсечката Γ_4 с начало точката $1 + iT_0$ и край $\eta + iT_0$,
- отсечката Γ_5 с начало точката $\eta + iT_0$ и край $\eta - iT_0$,
- отсечката Γ_6 с начало точката $\eta - iT_0$ и край $1 - iT_0$,
- отсечката Γ_7 с начало точката $1 - iT_0$ и край $1 - iT$,
- отсечката Γ_8 с начало точката $1 - iT$ и край $2 - iT$.

Контурът Γ е показан на следния чертеж.



Като използваме Лема 5.29 виждаме, че функцията $\Xi(s)$, определена чрез (388), е мероморфна вътре и по контура Γ, като има единствен полюс в точката $s=1$ и

$$Res_{s=1}\Xi(s) = \frac{x^2}{2}. \tag{395}$$

Тогава, като използваме теоремата за резидуумите, получаваме

$$\frac{1}{2\pi i}\int\limits_{\Gamma} \Xi(s)\,ds = \frac{x^2}{2}. \tag{396}$$

Да определим още:

- лъчът Γ_9 идващ от направлението $2-i\infty$ и с край точката $2-iT$,
- лъчът Γ_{10} с начало точката $2+iT$ и отиващ по направлението $2+i\infty$.

Тогава, като вземем предвид (389) и определението на Γ_1 виждаме, че

$$\Phi(x) = \frac{1}{2\pi i}\left(\int\limits_{\Gamma_9} \Xi(s)\,ds + \int\limits_{\Gamma_1} \Xi(s)\,ds + \int\limits_{\Gamma_{10}} \Xi(s)\,ds\right). \tag{397}$$

От (390), (396), (397) и от определенията на отсечките и лъчите $\Gamma_1,\ldots,\Gamma_{10}$ получаваме

$$R(x) = \Phi(x) - \frac{x^2}{2} = \frac{1}{2\pi i}\left(\int\limits_{\Gamma_9} \Xi(s)\,ds + \int\limits_{\Gamma_{10}} \Xi(s)\,ds - \sum_{k=2}^{8}\int\limits_{\Gamma_k} \Xi(s)\,ds\right),$$

следователно

$$|R(x)| \le \sum_{k=2}^{10}|R_k|, \qquad R_k = \int\limits_{\Gamma_k} \Xi(s)\,ds. \tag{398}$$

Първо ще оценим R_{10}. Като вземем предвид (388) намираме

$$R_{10}=i\int\limits_{T}^{\infty}\Xi(2+i\tau)\,d\tau=-i\int\limits_{T}^{\infty}\frac{\zeta'(2+i\tau)}{\zeta(2+i\tau)}\,\frac{x^{3+i\tau}}{(2+i\tau)(3+i\tau)}\,d\tau.$$

Оттук и от тъждеството (339) от Лема 5.28 получаваме

$$|R_{10}|\le\int\limits_{T}^{\infty}\left|\frac{\zeta'(2+i\tau)}{\zeta(2+i\tau)}\right|\frac{x^3}{\sqrt{4+\tau^2}\,\sqrt{9+\tau^2}}\,d\tau\le x^3\sum_{n=1}^{\infty}\frac{\Lambda(n)}{n^2}\int\limits_{T}^{\infty}\frac{d\tau}{\tau^2}\ll\frac{x^3}{T}.$$

Сега избираме

$$T=x\log x \tag{399}$$

и получаваме

$$R_{10}\ll\frac{x^2}{\log x}, \tag{400}$$

като константата в знака $\ll$ е абсолютна. По същия начин оценяваме R_9 и получаваме

$$R_9\ll\frac{x^2}{\log x}. \tag{401}$$

Сега да разгледаме R_2. Имаме

$$R_2=\int\limits_{2}^{1}\Xi(u+iT)\,du=-\int\limits_{2}^{1}\frac{\zeta'(u+iT)}{\zeta(u+iT)}\,\frac{x^{1+u+iT}}{(u+iT)(u+1+iT)}\,du,$$

откъдето

$$|R_2|\le\int\limits_{1}^{2}\left|\frac{\zeta'(u+iT)}{\zeta(u+iT)}\right|\,\frac{x^{1+u}}{\sqrt{u^2+T^2}\,\sqrt{(u+1)^2+T^2}}\,du.$$

От горното неравенство, от оценката в Лема 5.33 и от (399) следва

$$R_2\ll\log^9 T\int\limits_{1}^{2}\frac{x^{1+u}}{\sqrt{u^2+T^2}\,\sqrt{(u+1)^2+T^2}}\,du\ll\frac{x^3\,\log^9 T}{T^2}\ll\frac{x^2}{\log x}. \tag{402}$$

По аналогичен начин разглеждаме R_8 и намираме

$$R_8\ll\frac{x^2}{\log x}. \tag{403}$$

Да разгледаме R_3. Имаме

$$R_3=i\int\limits_{T}^{T_0}\Xi(1+i\tau)\,d\tau=i\int\limits_{T_0}^{T}\frac{\zeta'(1+i\tau)}{\zeta(1+i\tau)}\,\frac{x^{2+i\tau}}{(1+i\tau)(2+i\tau)}\,d\tau.$$

Оттук и от оценката в Лема 5.33 следва

$$|R_3| \leq \int_{T_0}^{T} \left| \frac{\zeta'(1+i\tau)}{\zeta(1+i\tau)} \right| \frac{x^2\, d\tau}{\sqrt{1+\tau^2}\,\sqrt{4+\tau^2}} \ll x^2 \int_{T_0}^{T} \frac{\log^9 \tau}{\tau^2}\, d\tau \ll x^2 \int_{T_0}^{\infty} \frac{d\tau}{\tau^{\frac{3}{2}}} \ll x^2 T_0^{-\frac{1}{2}}. \quad (404)$$

По същия начин работим и с величината R_7 и намираме

$$R_7 \ll x^2 T_0^{-\frac{1}{2}}. \quad (405)$$

За да продължим по-нататък, означаваме

$$\mathcal{M}(T_0) = \max_{s\in\Gamma^*} \left| \frac{\zeta'(s)}{\zeta(s)} \right|, \quad (406)$$

където Γ^* е обединението на отсечките Γ_4, Γ_5 и Γ_6.

Да разгледаме R_4. Имаме

$$R_4 = \int_{1}^{\eta} \Xi(u+iT_0)\, du = \int_{\eta}^{1} \frac{\zeta'(u+iT_0)}{\zeta(u+iT_0)} \frac{x^{1+u+iT_0}}{(u+iT_0)(1+u+iT_0)}\, du.$$

Оттук и от (406) следва

$$|R_4| \leq \mathcal{M}(T_0) \int_{\eta}^{1} \frac{x^{1+u}}{\sqrt{u^2+T_0^2}\,\sqrt{(1+u)^2+T_0^2}}\, du \leq \frac{\mathcal{M}(T_0)}{T_0^2} \int_{\eta}^{1} x^{1+u}\, du$$

и, тъй като

$$\int_{\eta}^{1} x^{1+u}\, du = \frac{x^2 - x^{1+\eta}}{\log x} \leq \frac{x^2}{\log x},$$

получаваме

$$|R_4| \leq \frac{\mathcal{M}(T_0)}{T_0^2} \frac{x^2}{\log x}.$$

Последното неравенство може да се запише във вида

$$R_4 \ll_{T_0} \frac{x^2}{\log x}. \quad (407)$$

(Константата в знака $\ll$ вече зависи от T_0). По аналогичен начин намираме

$$R_6 \ll_{T_0} \frac{x^2}{\log x}. \quad (408)$$

Остана да оценим R_5. Имаме

$$R_5 = i \int_{-T_0}^{T_0} \Xi(\eta+i\tau)\, d\tau = -i \int_{-T_0}^{T_0} \frac{\zeta'(\eta+i\tau)}{\zeta(\eta+i\tau)} \frac{x^{1+\eta+i\tau}}{(\eta+i\tau)(1+\eta+i\tau)}\, d\tau.$$

Тогава, като използваме (406) и си припомним, че η зависи от T_0, получаваме

$$|R_5| \le \mathcal{M}(T_0) x^{1+\eta} \int\limits_{-T_0}^{T_0} \frac{d\tau}{\sqrt{\eta^2+\tau^2}\,\sqrt{(1+\eta)^2+\tau^2}} \ll_{T_0} x^{1+\eta}.$$

Следователно, като вземем предвид (393) виждаме, че

$$R_5 \ll_{T_0} \frac{x^2}{\log x}. \tag{409}$$

От (400) – (403) и (407) – (409) следва, че съществува $A(T_0) > 0$, за което

$$|R_2| + |R_4| + |R_5| + |R_6| + |R_8| + |R_9| + |R_{10}| \le A(T_0)\frac{x^2}{\log x}.$$

Съответно от (404) и (405) получаваме

$$|R_3| + |R_7| \le B\,T_0^{-\frac{1}{2}}\,x^2,$$

където $B > 0$ е константа.

От горните две оценки и от (398) виждаме, че

$$|R(x)| \le A(T_0)\frac{x^2}{\log x} + B\,T_0^{-\frac{1}{2}}\,x^2. \tag{410}$$

Имаме избрано число $\varepsilon > 0$. Определяме $T_0 = T_0(\varepsilon)$ така, че

$$T_0 \ge 3 \qquad \text{и} \qquad B\,T_0^{-\frac{1}{2}} < \frac{\varepsilon}{2}. \tag{411}$$

За така определеното T_0 намираме $x_0 = x_0(\varepsilon)$ такова, че

$$x_0 > T_0 \tag{412}$$

и също така

$$\frac{A(T_0)}{\log x_0} < \frac{\varepsilon}{2}. \tag{413}$$

Тогава при $x \ge x_0$ за величината T, определена от (399), е налице изискването $T > T_0$, наложено в (392). От друга страна, от неравенството (413) следва, че при $x \ge x_0$ е изпълнено

$$A(T_0)\frac{x^2}{\log x} < \frac{\varepsilon}{2}x^2. \tag{414}$$

От (410), (411) и (414) следва (391), с което теоремата е доказана.

□

5.9 Характери на Дирихле

Характерите на Дирихле са аритметични функции с някои специални свойства (напълно мултипликативни, периодични и т.н.). В настоящите записки използваме алгебричен подход за тяхното определяне, като първо определяме понятието характер на произволна крайна абелева група.

Определение 5.39. *Нека G е крайна абелева група. Характер на групата G наричаме функция*

$$\chi : G \longrightarrow \mathbb{C}^* = \mathbb{C} \setminus \{0\},$$

за която

$$\chi(ab) = \chi(a)\chi(b) \qquad \text{за всеки} \qquad a, b \in G.$$

Множеството от характерите на G означаваме с $\widehat{G}$. Функцията

$$\chi_0 : G \longrightarrow \mathbb{C},$$

определена чрез

$$\chi_0(a) = 1 \qquad \text{за всяко} \qquad a \in G$$

наричаме главен характер на групата G.

В множеството $\widehat{G}$ въвеждаме умножение, като на всяка двойка $\chi_1, \chi_2 \in \widehat{G}$ съпоставим произведение $\chi_1\chi_2 \in \widehat{G}$, определено чрез $(\chi_1\chi_2)(a) = \chi_1(a)\chi_2(a)$. По-нататък, за всяко $\chi \in \widehat{G}$ определяме обратен елемент $\chi^{-1} \in \widehat{G}$ чрез формулата $\chi^{-1}(a) = (\chi(a))^{-1}$.

Някои най-прости свойства на характерите са изложени в следната

Лема 5.40. *Множеството $\widehat{G}$ с така въведените операции умножение и взимане на обратен елемент е крайна абелева група, чиято единица е главният характер χ_0. Ако $\chi \in \widehat{G}$, то са в сила следните свойства.*

(1) *Ако означим единицата на групата G с буквата e, то $\chi(e) = 1$.*

(2) *Ако $|G| = m$, то за всяко $a \in G$ числото $\chi(a)$ е m-ти корен на 1.*

(3) *За всяко $a \in G$ имаме $\chi(a^{-1}) = \chi(a)^{-1} = \overline{\chi(a)}$.*

Доказателство. Проверката на аксиомите за абелева група е тривиална. За да докажем свойство (1) използваме равенствата

$$\chi(e) = \chi(e^2) = \chi(e)^2$$

и, тъй като $\chi(e) \neq 0$, то $\chi(e) = 1$. По-нататък, щом групата G е от ред m. то $a^m = e$ за всяко $a \in G$. Тогава доказателството на (2) следва от равенствата

$$1 = \chi(e) = \chi(a^m) = (\chi(a))^m \,.$$

Да отбележим, че от свойство (2) следва, че $|\chi(a)| = 1$ за всяко $a \in G$. Оттук и от равенствата
$$1 = \chi(e) = \chi(aa^{-1}) = \chi(a)\chi(a^{-1})$$
следва верността на свойство (3).

Остана да съобразим, че групата $\widehat{G}$ е крайна. Това е вярно, тъй като всички характери са определени в крайното множество G и приемат стойности в крайното множество, състоящо се от корените на единицата от ред m.

□

Основна роля играе следната теорема.

Теорема 5.41. *Нека G е крайна абелева група и $\widehat{G}$ е съответната група от характери. Тогава е изпълнено равенството*
$$|\widehat{G}| = |G|. \tag{415}$$
Освен това, за всяко $a \in G, a \neq e$ съществува $\chi \in \widehat{G}$ такова, че $\chi(a) \neq 1$.

Доказателство. Ако $|G| = 1$, то твърдението е очевидно и оттук нататък ще считаме, че $|G| = m > 1$.

Нека H е подгрупа на G, като $H \neq G$. Означаваме $h = |H|$ и взимаме елемент $b \in G \setminus H$. Нека $t \in \mathbb{N}$ е най-малкото число, за което $b^t \in H$. (Такива числа съществуват, тъй като имаме, например, $b^m = e \in H$.)

Да разгледаме подгрупата H_1 на G, която се получава от H чрез присъединяване на елемента b. Както ще видим по-долу, тя се задава чрез формулата
$$H_1 = \{\ ab^l\ :\ a \in H,\ 0 \le l \le t-1\ \}. \tag{416}$$
Очевидно е, че горното множество съдържа както H, така и b. По-нататък, ако $a_1, a_2 \in H$ и $0 \le l_1, l_2 \le t-1$, то от равенството
$$a_1 b^{l_1} = a_2 b^{l_2} \tag{417}$$
следва $a_1 = a_2$ и $l_1 = l_2$. Наистина, ако допуснем, например, че $l_1 < l_2$, то от (417) получаваме $b^{l_2 - l_1} = a_1 a_2^{-1} \in H$. Но това е в противоречие с избора на t, тъй като $1 \le l_2 - l_1 \le t-1$. От горните разсъждения виждаме, че $|H_1| = ht$.

Сега ще проверим, че множеството (416) е подгрупа на G. Наистина, ако имаме $c_1, c_2 \in H_1$, записани във вида
$$c_j = a_j b^{l_j}, \qquad a_j \in H, \qquad 0 \le l_j \le t-1, \qquad j = 1, 2, \tag{418}$$
то
$$c_1 c_2 = ab^l, \qquad a = a_1 a_2 b^{\kappa t}, \quad l = l_1 + l_2 - \kappa t, \quad \kappa = \begin{cases} 0 & \text{ако } \ l_1 + l_2 \le t-1, \\ 1 & \text{ако } \ l_1 + l_2 \ge t. \end{cases} \tag{419}$$

Очевидно елементът a и числото l, определени от (419) удовлетворяват $a \in H$ и $0 \leq l \leq t-1$, следователно $c_1 c_2 \in H_1$. По аналогичен начин се проверява, че при $c \in H_1$ е изпълнено $c^{-1} \in H_1$.

И така, видяхме, че H_1 е подгрупата на G, породена от H и b, а от равенствата $h = |H|$, $ht = |H_1|$ следва, че числото t е равно на индекса на H в H_1, т.е.

$$t = [H_1 : H]. \tag{420}$$

Да вземем характер $\chi \in \widehat{H}$. Тъй като H е група от ред h и $b^t \in H$, то $b^{ht} = e$ и тогава

$$1 = \chi(e) = \chi(b^{th}) = \chi(b^t)^h.$$

От последното равенство виждаме, че $\chi(b^t)$ е корен на 1 от ред h, т.е.

$$\chi(b^t) = e\left(\frac{r}{h}\right) \qquad \text{за някое} \qquad r \in \mathbb{Z}. \tag{421}$$

(Тук и по-долу използуваме означението, зададено чрез формула (3).)

Да допуснем, че χ_1 е характер на H_1, който върху H съвпада с χ. Тъй като $b^t \in H$, като използуваме (421) получаваме

$$(\chi_1(b))^t = \chi_1\left(b^t\right) = \chi\left(b^t\right) = e\left(\frac{r}{h}\right).$$

Тогава $\chi_1(b)$ е корен от ред t от числото $e\left(\frac{r}{h}\right)$, откъдето

$$\chi_1(b) = e\left(\frac{r}{ht} + \frac{\nu}{t}\right) \qquad \text{за някое} \qquad \nu = 0, 1, \ldots, t-1.$$

От горните разсъждения заключаваме, че χ_1 съвпада с някоя от функциите

$$\chi^{(\nu)} : H_1 \longrightarrow \mathbb{C}^*, \qquad \nu = 0, 1, \ldots, t-1, \tag{422}$$

зададени чрез

$$\chi^{(\nu)}\left(ab^l\right) = \chi(a) e\left(\frac{(r + h\nu)l}{ht}\right) \qquad \text{при} \qquad a \in H, \ \ 0 \leq l \leq t-1. \tag{423}$$

Тези функции приемат ненулеви стойности и са две по две различни, тъй като числата $e\left(\frac{\nu}{t}\right)$, $\nu = 0, 1, \ldots .t-1$ са различните корени на 1 от ред t. Очевидно е също, че, за всяка от тях имаме $\chi^{(\nu)}(a) = \chi(a)$ при $a \in H$.

Сега ще се уверим, че всяка от функциите (422) е характер на H_1. Да вземем $c_1, c_2 \in H_1$ и да ги запишем във вида (418). Като използваме Лема 4.9 (3), (419) и

(423) намираме

$$\chi^{(\nu)}(c_1c_2) = \chi(a_1a_2b^{\kappa t})e\left(\frac{(r+h\nu)(l_1+l_2-\kappa t)}{ht}\right)$$

$$= \chi(a_1)\chi(a_2)\chi(b^{\kappa t})e\left(\frac{(r+h\nu)(l_1+l_2-\kappa t)}{ht}\right)$$

$$= \chi(a_1)\chi(a_2)\chi(b^t)^{\kappa}e\left(\frac{(r+h\nu)l_1}{ht}\right)e\left(\frac{(r+h\nu)l_2)}{ht}\right)e\left(-\frac{r\kappa}{h}\right).$$

Според (421) имаме $\chi(b^t)^{\kappa} = e\left(\frac{r\kappa}{h}\right)$, следователно, като използваме отново (418) и (423) получаваме

$$\chi^{(\nu)}(c_1c_2) = \chi^{(\nu)}(c_1)\chi^{(\nu)}(c_2).$$

И така, видяхме, че всяка от функциите (422) е характер на H_1, който продължава характера χ, а от друга страна, всяко продължение на χ върху H_1 съвпада с някоя от тези функции. Тогава всеки характер на H притежава точно t на брой продължения до характер на H_1. Оттук и от (420) получаваме равенството

$$|\widehat{H_1}| = |\widehat{H}| \cdot [H_1 : H]. \tag{424}$$

По-нататък, ако $H_1 \neq G$, към H_1 присъединяваме елемент от $G \setminus H_1$ и получаваме подгрупа H_2. След краен брой такива стъпки получаваме редица от подгрупи

$$H = H_0 \subset H_1 \subset H_2 \subset \cdots \subset H_j = G,$$

всяка от които се получава от предишната чрез присъединяване на нов елемент. При това са в сила равенствата

$$|\widehat{H_{i+1}}| = |\widehat{H_i}| \cdot [H_{i+1} : H_i], \qquad i = 0, 1, \ldots j-1.$$

Оттук непосредствено следва, че

$$|\widehat{G}| = |\widehat{H}| \cdot [G : H] \tag{425}$$

и, освен това, виждаме, че всеки характер на H се продължава до характер на G, като има точно $[G : H]$ такива продължения. Сега, ако приложим формула (425) при $H = \{e\}$ и използваме, че в този случай $|H| = |\widehat{H}| = 1$, получаваме (415).

Нека вземем произволно $a \in G, a \neq e$ и нека H е цикличната подгрупа на G, породена от a. Ясно е, че $|\widehat{H}| = |H| > 1$, следователно $\widehat{H}$, освен главния характер, ще съдържа поне още един характер χ. За него ще имаме $\chi(a) \neq 1$, тъй като в противен случай той би съвпадал с главния характер. Както видяхме по-горе, характерът χ може да се продължи до характер на групата G. С това теоремата е доказана.

$\square$

Теорема 5.42. *Нека G е крайна абелева група, като $|G| = m$ и нека $\widehat{G}$ е съответната група от характери. Тогава са изпълнени следните твърдения*

(1) *За всяко $a \in G$ имаме*

$$\sum_{\chi \in \widehat{G}} \chi(a) = \begin{cases} m & \textit{ако} \quad a = e, \\ 0 & \textit{ако} \quad a \neq e. \end{cases} \tag{426}$$

(2) *За произволни $a, b \in G$ имаме*

$$\sum_{\chi \in \widehat{G}} \chi(a)\overline{\chi(b)} = \begin{cases} m & \textit{ако} \quad a = b, \\ 0 & \textit{ако} \quad a \neq b. \end{cases} \tag{427}$$

(3) *За всяко $\chi \in \widehat{G}$ имаме*

$$\sum_{a \in G} \chi(a) = \begin{cases} m & \textit{ако} \quad \chi = \chi_0, \\ 0 & \textit{ако} \quad \chi \neq \chi_0. \end{cases} \tag{428}$$

Доказателство. Първо ще докажем свойство (1), което е частен случай на (2). Означаваме с S сумата в лявата страна на (426). Ако $a = e$, то като използваме Лема 5.40 (1) и Теорема 5.41 виждаме, че $S = m$. Нека сега $a \neq e$. Според Теорема 5.41 съществува характер $\chi^* \in \widehat{G}$ такъв, че $\chi^*(a) \neq 1$. Когато χ пробягва групата $\widehat{G}$, то $\chi\chi^*$ също пробягва тази група, следователно

$$S = \sum_{\chi \in \widehat{G}} (\chi\chi^*)(a) = \sum_{\chi \in \widehat{G}} \chi(a)\chi^*(a) = \chi^*(a)S.$$

Тъй като $\chi^*(a) \neq 1$, то от последното равенство следва $S = 0$, с което свойство (1) е доказано.

Сега да докажем (2). Ако T е сумата от лявата страна на (427), то като използуваме Лема 5.40 (3) и вече установеното свойство (1), получаваме

$$T = \sum_{\chi \in \widehat{G}} \chi(ab^{-1}) = \begin{cases} m & \text{ако} \quad ab^{-1} = e, \\ 0 & \text{ако} \quad ab^{-1} \neq e. \end{cases}$$

Оттук следва (427).

Накрая ще докажем (3). Означаваме с U сумата в лявата страна на (428). Ако $\chi = \chi_0$, то от определението на главен характер следва, че $U = m$. Ако пък $\chi \neq \chi_0$, то съществува $b \in G$, за което $\chi(b) \neq 1$. Когато a пробягва групата G, то ab също пробягва тази група, поради което

$$U = \sum_{a \in G} \chi(ab) = \sum_{a \in G} \chi(a)\chi(b) = \chi(b)U.$$

Като използуваме, че $\chi(b) \neq 1$, заключаваме, че $U = 0$, с което и свойство (2) е доказано.

$\square$

Сега ще определим понятието *характер на Дирихле* по зададен модул.

Определение 5.43. *Нека $q \in \mathbb{N}$. Характер на Дирихле по модул q се нарича всяка аритметична функция*

$$\chi : \mathbb{Z} \to \mathbb{C},$$

притежаваща свойствата:

(1) *χ е напълно мултипликативна, т.е.*

$$\chi(n_1 n_2) = \chi(n_1)\chi(n_2) \qquad \textit{за всеки} \qquad n_1, n_2 \in \mathbb{Z}.$$

(2) *χ е периодична с период q, т.е.*

$$\chi(n_1) = \chi(n_2) \qquad \textit{при} \qquad n_1 \equiv n_2 \pmod{q}.$$

(3) *$\chi(n) = 0$ при $(n, q) > 1$, $\qquad \chi(n) \neq 0$ при $(n, q) = 1$.*

Главен характер по модул q наричаме функцията χ_0, определена чрез

$$\chi_0(n) = \begin{cases} 1 & \textit{при} \quad (n, q) = 1, \\ 0 & \textit{при} \quad (n, q) > 1. \end{cases}$$

Ако характерът χ по модул q не съвпада с главния характер χ_0 по модул q ще казваме, че χ е неглавен характер.

Например, функцията, дефинирана с равенство (136) е неглавен характер по модул 4.

Основните свойства на характерите на Дирихле са събрани в следната теорема.

Теорема 5.44. *Нека $q \in \mathbb{N}$ и $\varphi(q)$ е функцията на Ойлер. В сила са следните свойства.*

(1) *Съществуват точно $\varphi(q)$ характери на Дирихле по модул q.*

(2) *Ако χ е характер на Дирихле по модул q, то за всяко $n \in \mathbb{Z}$, за което $(n, q) = 1$, стойността на $\chi(n)$ е корен на 1 от ред $\varphi(q)$.*

(3) *Ако χ е характер на Дирихле по модул q, то комплексно спрегнатата функция $\overline{\chi}$ също е характер на Дирихле по модул q. При това, ако $(a,q)=1$ и ако $\overline{a}$ е обратният елемент на a по модул q, т.е. решение на сравнението*

$$ax \equiv 1 \pmod q,$$

то имаме $\overline{\chi}(a) = \chi(\overline{a})$.

(4) *Ако $\sum_{\chi \pmod q}$ означава сума по всички характери на Дирихле по модул q, то за всяко $n \in \mathbb{Z}$ имаме*

$$\sum_{\chi \pmod q} \chi(n) = \begin{cases} \varphi(q) & \textit{при} \quad n \equiv 1 \pmod q, \\ 0 & \textit{при} \quad n \not\equiv 1 \pmod q. \end{cases}$$

(5) *Ако $a, n \in \mathbb{Z}$ и $(a,q)=1$, то*

$$\sum_{\chi \pmod q} \chi(n)\,\overline{\chi}(a) = \begin{cases} \varphi(q) & \textit{при} \quad n \equiv a \pmod q, \\ 0 & \textit{при} \quad n \not\equiv a \pmod q. \end{cases} \tag{429}$$

(6) *Ако $\sum_{n \pmod q}$ означава сума по произволна пълна система от остатъци по модул q, то*

$$\sum_{n \pmod q} \chi(n) = \begin{cases} \varphi(q) & \textit{при} \quad \chi = \chi_0, \\ 0 & \textit{при} \quad \chi \neq \chi_0. \end{cases} \tag{430}$$

(7) *Ако χ е неглавен характер по модул q, то при $y, z \in \mathbb{R}$, $y < z$ имаме*

$$\left| \sum_{y < n \le z} \chi(n) \right| \le \varphi(q). \tag{431}$$

Доказателство. За да докажем свойство (1) ще проверим, че характерите на Дирихле по модул q са във взаимно еднозначно съответствие с характерите на крайната абелева група

$$G = (\mathbb{Z}/q\mathbb{Z})^*\,, \tag{432}$$

състояща се от класовете $n^* = n + q\mathbb{Z}$, за които $(n,q)=1$. Нека G е групата (432) и $\chi^* \in \widehat{G}$. Определяме функцията $\chi : \mathbb{Z} \to \mathbb{C}$ по следния начин. При $n \in \mathbb{Z}$ полагаме

$$\chi(n) = \begin{cases} \chi^*(n^*) & \text{ако} \quad (n,q) = 1, \\ 0 & \text{ако} \quad (n,q) > 1. \end{cases}$$

Очевидно е, че тази функция удовлетворява свойствата от Определение 5.43. При това, на различни характери от $\widehat{G}$ съответстват различни характери на Дирихле по модул q. Накрая, ако χ е характер на Дирихле по модул q, то при $n^* = n + q\mathbb{Z}$, $(n,q)=1$ определяме χ^* чрез равенството $\chi^*(n^*) = \chi(n)$. Лесно се вижда, че тази дефиниция е коректна и, освен това, $\chi^* \in \widehat{G}$. (Проверката на последното твърдение оставяме на читателя.) Тъй като G е група от ред $\varphi(q)$, то от Теорема 5.41 следва, че съответната ѝ група от характери $\widehat{G}$ също е от ред $\varphi(q)$. С това свойство (1) е доказано.

Свойства (2) и (3) следват от Лема 5.40 (2), (3) и от описаното по-горе съответствие между характерите на Дирихле по модул q и характерите на групата (432). Аналогично, свойства (4) и (5) следват съответно от Теорема 5.42 (1) и (2).

Свойство (6) е следствие на Теорема 5.42 (3).

Остава да проверим свойство (7). За тази цел разделяме сумата $\sum_{y<n\le z}\chi(n)$ на краен брой суми, във всяка от които, без последната, сумирането е по q на брой последователни цели числа. Според свойство (6) всяка от тези суми е равна на нула. Последната сума е по целите числа от интервал с дължина по-малка от q и съдържа не повече от $\varphi(q)$ на брой различни от нула събираеми, като модулът на всяко от тях е равен на 1. Следователно модулът на тази сума не надхвърля $\varphi(q)$, с което свойство (7) е доказано.

$\square$

5.10 L-функции на Дирихле

Определение 5.45. *Нека $q\in\mathbb{N}$ и нека χ е характер на Дирихле по модул q. Редът на Дирихле*

$$L(s,\chi)=\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s} \tag{433}$$

се нарича L-функция на Дирихле, отговаряща на характера χ.

Лема 5.46. *Всяка L-функция на Дирихле $L(s,\chi)$ е аналитична при $Re(s)>1$. В тази област редът (433) може да се диференцира почленно, т.е. за всяко $k\in\mathbb{N}$ имаме*

$$L^{(k)}(s,\chi)=\sum_{n=1}^{\infty}\frac{\chi(n)\,(-\log n)^k}{n^s}. \tag{434}$$

В сила тъждеството

$$L(s,\chi)=\prod_p\left(1-\frac{\chi(p)}{p^s}\right)^{-1}, \tag{435}$$

където произведението е взето по всички прости числа. Освен това имаме

$$L(s,\chi)\ne 0 \qquad \textit{при} \qquad Re(s)>1.$$

Доказателство. Използуваме се Теорема 3.45 и Лема 5.18 и разсъждаваме както при доказателствата на Лема 5.25, Лема 5.26 и Лема 5.27. Подробностите оставяме на читателя.

$\square$

Лема 5.47. *За всяка L-функция на Дирихле $L(s,\chi)$ е в сила тъждеството*

$$-\frac{L'(s,\chi)}{L(s,\chi)}=\sum_{n=1}^{\infty}\frac{\Lambda(n)\chi(n)}{n^s} \qquad \textit{при} \qquad Re(s)>1. \tag{436}$$

Доказателство. Умножаваме по правилото от Лема 5.23 реда на Дирихле $L(s,\chi)$, зададен чрез (433) и реда на Дирихле от дясната страна на (436). Използваме Лема 3.42 и това, че всеки характер на Дирихле е напълно мултипликативна функция. След прости преобразования, които предоставяме на читателя, получаваме реда $\sum_{n=1}^{\infty} \frac{\chi(n)\log n}{n^s}$, който според Лема 5.46 представя функцията $-L'(s,\chi)$.

$\square$

Както ще видим от следващите твърдения, аналитичните свойства на $L(s,\chi)$ зависят съществено от това дали характерът χ е главен или неглавен. От следващата лема ще се убедим, че изследването на $L(s,\chi_0)$ е по същество еквивалентно на изследването на дзета-функцията на Риман $\zeta(s)$.

Лема 5.48. *Ако χ_0 е главният характер по модул q, то*

$$L(s,\chi_0) = \zeta(s) \prod_{p|q} \left(1 - \frac{1}{p^s}\right) \qquad \text{при} \qquad Re(s) > 1. \tag{437}$$

Функцията $L(s,\chi_0)$ прижава мероморфно продължение в $Re(s) > 0$, като има полюс само в точката $s = 1$. Този полюс е прост и е с резидуум равен на $\frac{\varphi(q)}{q}$.

Доказателство. Като използваме формула (435) и определението на главния характер, получаваме

$$L(s,\chi_0) = \prod_{p} \left(1 - \frac{\chi_0(p)}{p^s}\right)^{-1} = \prod_{p\nmid q} \left(1 - \frac{1}{p^s}\right)^{-1}.$$

От горното равенство и от тъждеството (336) за $\zeta(s)$ получаваме (437).

От Лема 5.29 знаем, че $\zeta(s)$ се продължава до мероморфна функция в $Re(s) > 0$, с полюс само в точката $s = 1$, като този полюс е прост и е с резидуум 1. Тогава равенството (437) ни дава мероморфно продължение на $L(s,\chi_0)$ в полуравнината $Re(s) > 0$, като тази функция има прост полюс в $s = 1$ с резидуум равен на

$$\prod_{p|q} \left(1 - \frac{1}{p}\right) = \frac{\varphi(q)}{q}.$$

$\square$

Сега ще се заемем с изучаването на $L(s,\chi)$ когато $\chi \neq \chi_0$.

Лема 5.49. *Нека χ е неглавен характер по модул q. Тогава редът (433), определящ функцията $L(s,\chi)$ е сходящ при $\sigma = Re(s) > 0$ и при всяко $x \geq 1$ имаме*

$$\left| L(s,\chi) - \sum_{n \leq x} \frac{\chi(n)}{n^s} \right| \leq \varphi(q)|s|\,\sigma^{-1}\,x^{-\sigma}. \tag{438}$$

Доказателство. Прилагаме преобразованието на Абел (Лема 2.1) и получаваме, че за произволни $x, y \in \mathbb{R}$, $0 < x < y$ имаме

$$\sum_{x<n\le y} \frac{\chi(n)}{n^s} = y^{-s} \sum_{x<n\le y} \chi(n) - \int\limits_x^y \left(\sum_{x<n\le t} \chi(n) \right) \frac{d}{dt} \left(t^{-s}\right) \, dt$$

$$= y^{-s} \sum_{x<n\le y} \chi(n) + s \int\limits_x^y \left(\sum_{x<n\le t} \chi(n) \right) \frac{dt}{t^{s+1}}.$$

Тогава, като приложим неравенството на триъгълника и неравенството (431) от Теорема 5.44 (7), получаваме

$$\left| \sum_{x<n\le y} \frac{\chi(n)}{n^s} \right| \le \varphi(q) \left(y^{-\sigma} + |s| \int\limits_x^y \frac{dt}{t^{\sigma+1}} \right) = \varphi(q) \left(y^{-\sigma} + |s| \frac{x^{-\sigma} - y^{-\sigma}}{\sigma} \right).$$

Оттук непосредствено следва

$$\left| \sum_{x<n\le y} \frac{\chi(n)}{n^s} \right| \le \varphi(q) |s| \, \sigma^{-1} \, x^{-\sigma}. \tag{439}$$

От горната формула и от критерия на Коши за сходимост на безкраен ред следва, че при $\sigma = Re(s) > 0$ редът $L(s, \chi)$ е сходящ. В неравенството (439) извършваме граничен преход $y \to \infty$ и получаваме (438).

□

В следващата теорема е формулирано едно от най-важните свойства на L-функциите на Дирихле. Както ще видим, то е в основата на доказателството на теоремата на Дирихле за простите числа в аритметични прогресии.

Теорема 5.50. *Ако χ е неглавен характер по модул q, то $L(1, \chi) \neq 0$.*

Доказателство. Първо ще докажем твърдението в случая, когато χ е комплексен характер (т.е приема поне една стойност, която не е реално число). При $Re(s) > 1$ разглеждаме реда на Дирихле

$$\mathcal{F}(s) = \sum_{\substack{n=1 \\ n\equiv 1 \pmod q}}^{\infty} \frac{\Lambda(n)}{n^s}. \tag{440}$$

Очевидно, за указаните стойности на s горният ред е сходящ. Да отбележим, че

$$\mathcal{F}(s) \ge 0 \qquad \text{при реално} \qquad s > 1. \tag{441}$$

Използуваме Теорема 5.44 (4) и Лема 5.47 и получаваме

$$\mathcal{F}(s) = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s} \frac{1}{\varphi(q)} \sum_{\chi \pmod q} \chi(n)$$

$$= \frac{1}{\varphi(q)} \sum_{\chi \pmod q} \sum_{n=1}^{\infty} \frac{\Lambda(n)\chi(n)}{n^s}$$

$$= -\frac{1}{\varphi(q)} \sum_{\chi \pmod q} \frac{L'(s,\chi)}{L(s,\chi)}.$$

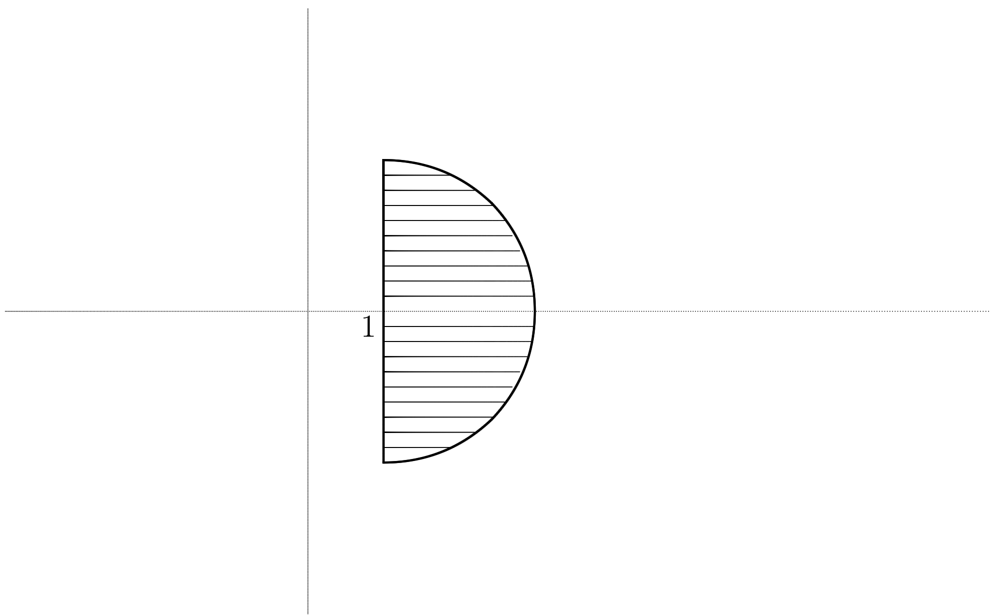
Отделяме събираемото, съответстващо на главния характер χ_0, и записваме горното равенство във вида

$$\mathcal{F}(s) = -\frac{1}{\varphi(q)} \frac{L'(s,\chi_0)}{L(s,\chi_0)} - \frac{1}{\varphi(q)} \sum_{\substack{\chi \pmod q \\ \chi \neq \chi_0}} \frac{L'(s,\chi)}{L(s,\chi)}. \tag{442}$$

От тъждеството (437) от Лема 5.48 следва

$$-\frac{L'(s,\chi_0)}{L(s,\chi_0)} = -\frac{\zeta'(s)}{\zeta(s)} - \sum_{p|q} \frac{\log p}{p^s - 1}. \tag{443}$$

Но според Лема 5.29 функцията $\zeta(s)$ притежава прост полюс в точката $s = 1$, следователно функцията $-\frac{\zeta'(s)}{\zeta(s)}$ има прост полюс с резидуум 1 в същата точка. Освен това второто събираемо в дясната част на (443) е ограничено в околност на точката $s = 1$. Тогава в сечението на полуравнината $Re(s) > 1$ с някаква околност на $s = 1$ (виж чертежа)



имаме
$$-\frac{L'(s,\chi_0)}{L(s,\chi_0)} = \frac{1}{s-1} + O(1). \tag{444}$$
Да отбележим, че оттук нататък константите в знаците O и $\ll$ зависят от q.

Разглеждаме сумата по неглавните характери в дясната страна на равенство (442). Събираемите, отговарящи на характери χ, за които $L(1,\chi) \neq 0$ са ограничени в околност на $s = 1$, тъй като в такава околност знаменателите на съответните функции са аналитични функции, които не се анулират. Следователно, като вземем предвид (444), виждаме, че в сечението на полуравнината $Re(s) > 1$ с някаква околност на $s = 1$ (виж последния чертеж) е изпълнено

$$\mathcal{F}(s) = \frac{1}{\varphi(q)(s-1)} - \frac{1}{\varphi(q)} \sum_{\substack{\chi \pmod q \\ L(1,\chi)=0}} \frac{L'(s,\chi)}{L(s,\chi)} + O(1). \tag{445}$$

(Условието $\chi \neq \chi_0$ е пропуснато, тъй като $L(s,\chi_0)$ притежава полюс в $s = 1$, следователно не може да има нула в същата точка.)

Да допуснем, че $\chi \neq \chi_0$ е характер, за който $L(1,\chi) = 0$ (нашата цел е да се убедим, че такива не съществуват) и нека k_χ е кратността на нулата на $L(s,\chi)$ в точката $s = 1$. Тогава функцията $\frac{L'(s,\chi)}{L(s,\chi)}$ притежава прост полюс с резидуум k_χ в същата точка, следователно в нейна околност е изпълнено

$$\frac{L'(s,\chi)}{L(s,\chi)} = \frac{k_\chi}{s-1} + O(1).$$

От последната формула и от (445) следва, че в множество от вида показан на чертежа имаме

$$\mathcal{F}(s) = \frac{1}{\varphi(q)(s-1)} \left(1 - \sum_{\substack{\chi \pmod q \\ L(1,\chi)=0}} k_\chi \right) + O(1). \tag{446}$$

Ако допуснем, че χ е комплексен характер, за който $L(1,\chi) = 0$, то $\overline{\chi}$ е комплексен характер, различен от χ, като при това имаме

$$L(1,\overline{\chi}) = \sum_{n=1}^{\infty} \frac{\overline{\chi(n)}}{n} = \overline{\sum_{n=1}^{\infty} \frac{\chi(n)}{n}} = \overline{L(1,\chi)} = 0.$$

Но тогава сумата по характерите в (446) ще съдържа поне две събираеми. Оттук следва, че изразът в скобите в (446) няма да надхвърля $1 - k_\chi - k_{\overline{\chi}} < 0$, следователно този израз ще е отрицателен. От това съображение и от формула (446) получаваме

$$\mathcal{F}(s) \to -\infty \qquad \text{при} \qquad s \to 1 + 0,$$

а последното противоречи на (441). И така, ако допуснем, че за някой комплексен характер χ е изпълнено $L(1,\chi) = 0$, получаваме противоречие. Следователно за всеки комплексен характер имаме $L(1,\chi) \neq 0$.

От изложеното по-горе разсъждение следва също, че би могло да има най-много един реален характер χ, за който $L(1,\chi)=0$. Остава да установим, че всъщност няма нито един такъв.

Да допуснем, че $\chi \neq \chi_0$ е реален характер, такъв че $L(1,\chi)=0$. При произволно $x>1$ разглеждаме сумата

$$T(x)=\sum_{n\le x}\tau_\chi(n)\,n^{-\frac{1}{2}}, \tag{447}$$

където

$$\tau_\chi(n)=\sum_{d|n}\chi(d). \tag{448}$$

Според Лема 3.30 функцията $\tau_\chi(n)$ е мултипликативна и, ако каноничното развитие на n е

$$n=p_1^{k_1}\dots p_m^{k_m}, \tag{449}$$

то

$$\tau_\chi(n)=\prod_{j=1}^{m}\tau_\chi(p_j^{k_j}), \qquad \tau_\chi(p_j^{k_j})=1+\chi(p_j)+\chi(p_j)^2+\dots\chi(p_j)^{k_j}. \tag{450}$$

Да отбележим, че според Теорема 5.44 (2), стойностите, които може да приема реалният характер χ, са само числата 0, 1 и -1.

Ако $\chi(p_j)=0$, то $\tau_\chi(p_j^{k_j})=1$.

Ако $\chi(p_j)=1$, то $\tau_\chi(p_j^{k_j})=k_j+1\ge 1$.

Ако пък $\chi(p_j)=-1$, то

$$\tau_\chi(p_j^{k_j})=1-1+1-\dots+(-1)^{k_j}=\begin{cases}0 & \text{при} \quad k_j\equiv 1 \pmod 2,\\ 1 & \text{при} \quad k_j\equiv 0 \pmod 2.\end{cases}$$

Оттук следва, че винаги е изпълнено $\tau_\chi(p_j^{k_j})\ge 0$ и, като вземем предвид (450) виждаме, че

$$\tau_\chi(n)\ge 0 \qquad \text{при} \qquad n\in\mathbb{N}. \tag{451}$$

Нека сега $n=m^2$ за някое $m\in\mathbb{N}$. Тогава всички числа k_j от формула (449) са четни, следователно $\tau_\chi(p_j^{k_j})\ge 1$. Тогава получаваме

$$\tau_\chi(n)\ge 1 \qquad \text{при} \qquad n=m^2, \qquad m\in\mathbb{N}. \tag{452}$$

От (447), (451), (452) и Лема 2.6 (3) следва

$$T(x)\ge \sum_{\substack{n\le x\\ n=m^2,\ m\in\mathbb{N}}}\frac{1}{\sqrt{n}}=\sum_{m\le\sqrt{x}}\frac{1}{m}\gg \log x. \tag{453}$$

От друга страна, като използуваме (447) и (448) получаваме

$$T(x) = \sum_{n\le x} \sum_{d|n} \chi(d)\, n^{-\frac{1}{2}} = \sum_{n\le x} \sum_{md=n} \chi(d)\, n^{-\frac{1}{2}} = \sum_{md\le x} \chi(d)\,(md)^{-\frac{1}{2}} = T_1 + T_2, \quad (454)$$

където в T_1 са събираемите, за които $d \le \sqrt{x}$, а сумата T_2 съдържа останалите събираеми.

Да разгледаме T_1. Като използуваме определението на тази сума и формула (12) намираме

$$T_1 = \sum_{\substack{md\le x\\ d\le\sqrt{x}}} \chi(d)\,(md)^{-\frac{1}{2}} = \sum_{d\le\sqrt{x}} \chi(d)\, d^{-\frac{1}{2}} \sum_{m\le\frac{x}{d}} m^{-\frac{1}{2}}$$

$$= \sum_{d\le\sqrt{x}} \chi(d)\, d^{-\frac{1}{2}} \left(\frac{1}{2}\left(\frac{x}{d}\right)^{\frac{1}{2}} + c + O\left(\left(\frac{d}{x}\right)^{\frac{1}{2}}\right)\right)$$

$$= \frac{1}{2}x^{\frac{1}{2}} \sum_{d\le\sqrt{x}} \frac{\chi(d)}{d} + c \sum_{d\le\sqrt{x}} \frac{\chi(d)}{\sqrt{d}} + O(1). \quad (455)$$

Но според оценката (438) от Лема 5.49 имаме

$$\sum_{d\le\sqrt{x}} \frac{\chi(d)}{d} = L(1,\chi) + O\left(x^{-\frac{1}{2}}\right),$$

$$\sum_{d\le\sqrt{x}} \frac{\chi(d)}{\sqrt{d}} = L(1/2,\chi) + O(x^{-\frac{1}{4}}) = O(1).$$

От горните формули и от (455) следва

$$T_1 = \frac{1}{2}\, L(1,\chi)\, x^{\frac{1}{2}} + O(1). \quad (456)$$

Сега да разгледаме сумата T_2. Имаме

$$T_2 = \sum_{\substack{md\le x\\ \sqrt{x}<d\le x}} \chi(d)\,(md)^{-\frac{1}{2}} = \sum_{m\le\sqrt{x}} m^{-\frac{1}{2}} \sum_{\sqrt{x}<d\le\frac{x}{m}} \chi(d)\, d^{-\frac{1}{2}}.$$

Като вземем предвид оценката (439), получена при доказателство на Лема 5.49 и също Лема 2.6 (1), намираме

$$T_2 \ll x^{-\frac{1}{4}} \sum_{m\le\sqrt{x}} m^{-\frac{1}{2}} \ll 1. \quad (457)$$

От (454), (456) и (457) следва

$$T(x) = \frac{1}{2}\, L(1,\chi)\, x^{\frac{1}{2}} + O(1).$$

Но тогава от допускането $L(1,\chi) = 0$ се получава

$$T(x) = O(1),$$

а горната оценка противоречи на неравенството (453).

С това се убеждаваме, че за всеки реален неглавен характер χ е изпълнено $L(1,\chi) \neq 0$, с което теоремата е доказана.

$\square$

5.11 Теорема на Дирихле за простите числа в аритметична прогресия

Вече разполагаме с всички помощни резултати, необходими за доказателството на класическата теорема на Дирихле. Остава да изложим формулировката и доказателството ѝ.

Теорема 5.51 (Дирихле)**.** *Ако $a \in \mathbb{Z}$, $q \in \mathbb{N}$ и $(a,q) = 1$, то аритметичната прогресия*

$$a + kq, \qquad k = 0, 1, 2, 3, \ldots$$

съдържа безбройно много прости числа.

Доказателство. При $Re(s) > 1$ разглеждаме сумата

$$\mathcal{B} = \sum_{\substack{n=1 \\ n \equiv a \pmod q}}^{\infty} \frac{\Lambda(n)}{n^s}. \tag{458}$$

От Определение 3.22 виждаме, че

$$\mathcal{B} = \sum_{p \equiv a \pmod q} \frac{\log p}{p^s} + \Delta, \tag{459}$$

където

$$\Delta = \sum_{\substack{k \geq 2,\, p \\ p^k \equiv a \pmod q}} \frac{\log p}{p^{ks}}.$$

Ясно е, че

$$|\Delta| \leq \sum_{\substack{k \geq 2,\, p \\ p^k \equiv a \pmod q}} \frac{\log p}{p^k} \leq \sum_p \log p \sum_{k=2}^{\infty} p^{-k} = \sum_p \frac{\log p}{p(p-1)} \ll 1.$$

От горната оценка и от (459) следва

$$\mathcal{B} = \sum_{p \equiv a \pmod q} \frac{\log p}{p^s} + O(1) \qquad \text{при} \qquad Re(s) > 1. \tag{460}$$

От друга страна, от (458), от Теорема 5.44 (5) и от Лема 5.47 получаваме

$$\begin{aligned}
\mathcal{B} &= \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s} \, \frac{1}{\varphi(q)} \sum_{\chi \pmod q} \chi(n) \, \overline{\chi(a)} \\
&= \frac{1}{\varphi(q)} \sum_{\chi \pmod q} \overline{\chi(a)} \sum_{n=1}^{\infty} \frac{\Lambda(n)\chi(n)}{n^s} \\
&= -\frac{1}{\varphi(q)} \sum_{\chi \pmod q} \overline{\chi(a)} \, \frac{L'(s,\chi)}{L(s,\chi)} \\
&= -\frac{1}{\varphi(q)} \frac{L'(s,\chi_0)}{L(s,\chi_0)} - \frac{1}{\varphi(q)} \sum_{\substack{\chi \pmod q \\ \chi \neq \chi_0}} \overline{\chi(a)} \, \frac{L'(s,\chi)}{L(s,\chi)}
\end{aligned} \tag{461}$$

Но при $\chi \neq \chi_0$ според Теорема 5.50 имаме $L(1,\chi) \neq 0$, следователно функцията $\frac{L'(s,\chi)}{L(s,\chi)}$ е аналитична в околност на точката $s = 1$. Оттук следва, че всяко от събираемите в сумата от дясната страна на (461) е ограничено в сечението на полуравнината $Re(s) > 1$ с някаква околност на точката $s = 1$ (виж чертежа на стр. 128). Тогава в това множество имаме

$$\mathcal{B} = -\frac{1}{\varphi(q)} \frac{L'(s,\chi_0)}{L(s,\chi_0)} + O(1).$$

Сега, като използваме формула (444), получена в процеса на доказателството на Теорема 5.50, виждаме, че в сечението на полуравнината $Re(s) > 1$ с околност на $s = 1$ е изпълнено

$$\mathcal{B} = \frac{1}{\varphi(q)(s-1)} + O(1).$$

В частност, при реално $s > 1$ получаваме

$$\mathcal{B} \to \infty \qquad \text{при} \qquad s \to 1 + 0. \tag{462}$$

От (460) и (462) следва, че

$$\sum_{p \equiv a \pmod q} \frac{\log p}{p^s} \to \infty \qquad \text{при} \qquad s \to 1 + 0.$$

Тогава съществуват безбройно много прости числа p, удовлетворяващи сравнението $p \equiv a \pmod q$. С това теоремата е доказана.

$\square$

Литература

[1] И.М.Виноградов, *Основы теории чисел*, Москва, „Наука", 1981.

[2] А.И.Галочкин, Ю.Ф.Нестеренко, А.Б.Шидловский *Введение в теорию чисел*, Москва, Изд. Моск. университетата, 1984.

[3] А.А.Карацуба, *Основы аналитической теории чисел*, Москва, „Наука", 1983.

[4] Е.Титчмарш, *Теория функций*, Москва, „Наука", 1980.

[5] К.Чандрасекхаран, *Введение в аналитическую теорию чисел*, Москва, „Мир", 1974.

[6] G.H.Hardy, E.M.Wright, *An introduction to the theory of numbers*, Fifth ed. Oxford Univ. Press, 1979.

[7] H.Iwaniec, E.Kowalski, *Analytic number theory*, Amer. Math. Soc., Colloquium Publications, 53, 2004

[8] G.Tenenbaum, *Introduction to analytic and probabilistic number theory*, Cambridge Univ. Press, 2004.

[9] E.C.Titchmarsh, *The Theory of the Riemann Zeta-Function*, (revised by D.R.Heath-Brown), Oxford Univ. Press, 1987.