Нако Начев **Дойчин Толев**

Ръководство по теория на числата

Предговор

Целта на настоящото ръководство е да запознае читателя с някои основни понятия и теореми от елементарната теория на числата — делимост, разлагане на прости множители, числови функции и свойствата им, сравнения, теореми на Чебишев за разпределение на простите числа.

В ръководството е изложена част от теорията под форма на поредица от определения и задачи. Твърденията в някои от задачите представляват основни теореми от теорията на числата, в други задачи се дават примери, поясняващи теоремите. Има също голям брой чисто технически задачи, предназначението на които е да спомогне за придобиването на изчислителни умения и за по–доброто разбиране на определенията и методите.

В редица случаи (предимно когато разглеждания материал съвпада или частично се припокрива с този от други, лесно достъпни източници) решенията са пропуснати, дадени са съвсем накратко или пък са предложени други, по–малко известни, методи за решаване. В част от задачите са формулирани и доказани резултати, които до този момент не са разглеждани в родната литература.

В забележките е дадена допълнителна информация, а също и някои исторически данни. Задачите и определенията имат различна номерация. На места са номерирани и формули, като номерацията се отнася само за съответната задача, нейното решение и забележките към нея.

Предполага се, че читателят е запознат с елементарната алгебра и с основите на математическия анализ. Ръководството е предназначено главно за студенти от математическите специалности на университетите, но би било полезно за учители по математика, докторанти и за всички интересуващи се от теорията на числата.

Авторите изразяват своята дълбока благодарност на рецензентите проф. д.м.н. Тодор Ж. Моллов и проф. д–р Петко Д. Пройнов за положения труд при четенето на ръкописа и за ценните препоръки за подобряване на изложението.

Означения

Основни числови множества:

$\mathbb{N}$ – множеството на естествените числа,
$\mathbb{Z}$ – пръстенът на целите числа,
$\mathbb{Q}$ – полето на рационалните числа,
$\mathbb{Q}_p$ – полето на p–адичните числа – опр. 13,
$\mathbb{R}$ – полето на реалните числа,
$\mathbb{C}$ – полето на комплексните числа.

Числови функции:

$\mathrm{ord}_p n$ – опр. 8,
$\overline{(k)}_n$ – опр.42,
$\omega(n)$ – брой на различните прости делители на n – опр. 24,
$\Omega(n)$ – брой на всички прости множители в каноничното разлагане на n – опр. 24,
$\mu(n)$ – функция на Мьобиус – опр. 25, зад. 111,
$\lambda(n)$ – функция на Лиувил – опр. 26, зад. 119,
$\Lambda(n)$ – функция на Манголд – опр. 27, зад. 123,
$\varphi(n)$ – функция на Ойлер (индикатор) – опр. 28,
$\tau(n)$ – брой на делителите на n – опр. 29,
$\tau_k(n)$ – обобщение на $\tau(n)$ – опр. 30,
$\sigma(n)$ – сума на делителите на n – опр. 31,
$\sigma_\alpha(n)$ – обобщение на $\sigma(n)$ – опр. 31,
$r_f(n)$ – брой на решенията на сравнението $f(x) \equiv 0 \pmod{n}$ – опр. 38.

Функции на реален аргумент:

$[x]$ – цяла част на x – опр. 15,
$\{x\}$ – дробна част на x – опр. 15,
$\rho_1(x)$ – опр. 16,
$\rho_2(x)$ – опр. 17,
$e(x)$ – опр. 39,
$\pi(x)$ – брой на простите числа, не надминаващи x – опр. 44,
$\theta(x)$ – функция на Чебишев – опр. 44,
$\psi(x)$ – функция на Чебишев – опр. 44.

Функции, дефинирани в $\mathbb{Q}$:

$\mathrm{ord}_p r$	–	опр. 10,
$\|\|r\|\|_p$	–	p–адична норма на r – опр. 12,
$\rho_p(r_1, r_2)$	–	p–адично разстояние – зад. 59.

Функции на комплексен аргумент:

$Re\, s$	–	реална част на s,
$Im\, s$	–	имагинерна част на s,
$\zeta(s)$	–	дзета–функция на Риман – опр. 32.

Аритметични суми:

$c(n, a)$	–	сума (функция) на Раманудджан – опр. 40,
$S_l(n, a)$	–	сума на Х. Вайл – опр. 41,
$S_l^*(n, a)$	–	сума на Х. Вайл – опр. 41,
$K(n; a, b)$	–	сума на Клостерман – опр. 43.

Прости числа:

Буквата p винаги се използува за означаване на прости числа.

Суми и произведения:

$\sum_{a<n\le b} f(n)$	–	сума по всички $n \in \mathbb{Z}$, за които $a < n \le b$,
$\sum_{n\le b} f(n)$	–	сума по всички $n \in \mathbb{N}$, за които $n \le b$,
$\prod_{a<n\le b} f(n)$	–	произведение по $n \in \mathbb{Z}$, за които $a < n \le b$,
$\prod_{n\le b} f(n)$	–	произведение по $n \in \mathbb{N}$, за които $n \le b$,
$\sum_{p\le b} f(p)$	–	сума по всички прости числа $p \le b$,
$\prod_{p\le b} f(p)$	–	произведение по всички прости числа $p \le b$,
$\sum_p f(p)$	–	сума по всички прости числа,
$\prod_p f(p)$	–	произведение по всички прости числа.

Символ на Ландау:

Формулата $f(x) = \mathcal{O}\big(g(x)\big)$ означава, че съществуват $c > 0$ и x_0, такива че при $x \ge x_0$ е изпълнено $|f(x)| \le c\, g(x)$. Тук $f(x)$ и $g(x)$ са функции, дефинирани при достатъчно големи $x \in \mathbb{R}$, като $f(x)$, най–общо казано, е комплекснозначна, а $g(x) > 0$.

Съдържание

1 Делимост на числата

Основни понятия за делимост

Задача 1. Да се докаже, че следните три твърдения са еквивалентни:

а) Ако M е непразно подмножество на $\mathbb{N}$, то M съдържа най–малък елемент.

б) Ако множеството $M \subset \mathbb{N}$ притежава свойствата

1) $1 \in M$,

2) $n \in M \Longrightarrow n+1 \in M$,

то $M = \mathbb{N}$.

в) Всяка строго намаляваща редица от естествени числа е крайна.

Забележка: Задача 1 има помощен характер за настоящия раздел. В нея са формулирани три фундаментални свойства на множеството $\mathbb{N}$ на естествените числа, които се използуват във всички раздели на математиката. Решението е пропуснато тъй като то може да бъде намерено без особени усилия от читателя.

Твърденията от задача 1 са известни, съответно, под названията *Принцип на добрата наредба*, *Принцип на математическата индукция* и *Принцип за прекъсване на строго намаляващите редици*.

Определение 1. Нека $a, b \in \mathbb{Z}$, $b \neq 0$. Казваме, че a *се дели на* b и пишем $b \mid a$, ако съществува $c \in \mathbb{Z}$, такова че $a = bc$. Числото a се нарича *кратно* на b, b се нарича *делител* на a. Когато a не се дели на b употребяваме означението $b \nmid a$.

Забележка: По–нататък, при наличие на условието $b \mid a$ ще подразбираме, че $a, b \in \mathbb{Z}$ и $b \neq 0$.

Задача 2. Да се докаже, че за релацията делимост са в сила следните свойства:

а) Ако $a \in \mathbb{Z}$, $a \neq 0$, то $a \mid a$.

б) Ако $a, b \in \mathbb{N}$, $a \mid b$ и $b \mid a$, то $a = b$.

в) Ако $a, b, c \in \mathbb{Z}$, $a \mid b$ и $b \mid c$, то $a \mid c$.

г) Ако $a, b \in \mathbb{Z}$, $a \mid b$ и $b \mid a$, то $|a| = |b|$.

д) Ако $a, b \in \mathbb{N}$ и $a \mid b$, то $a \leq b$.

е) Ако $a, b \in \mathbb{Z}$, $ab \neq 0$ и $a \mid b$, то $|a| \leq |b|$.

ж) Ако $a, b \in \mathbb{Z}$ и $a \mid b$, то $-a \mid b$.

з) Ако $a, b, c \in \mathbb{Z}$ и $a \mid b$, то $a \mid bc$.

и) Ако $a, b, c \in \mathbb{Z}$, $a \mid b$ и $a \mid c$, то $a \mid (b \pm c)$.

Теорема за деление с частно и остатък. Нека $a \in \mathbb{Z}$ и $m \in \mathbb{N}$. Съществуват еднозначно определени $q, r \in \mathbb{Z}$, такива че $a = mq + r$ и $0 \leq r < m$.

Задача 3. Да се докаже теоремата за деление с частно и остатък.

Решение: Очевидно съществува $q \in \mathbb{Z}$, такова че числото a лежи в интервала $[qm, (q+1)m)$. Тогава $a = mq + r$ за някое r, намиращо се измежду числата $0, 1, \ldots m-1$. Единствеността на представянето следва от това, че интервалите $[qm, (q+1)m)$, където $q \in \mathbb{Z}$, два по два не се пресичат.

Определение 2. Нека $a \in \mathbb{Z}$, $m \in \mathbb{N}$ и нека a е представено във вида $a = mq + r$, където $q, r \in \mathbb{Z}$ и $0 \leq r < m$. Числата q и r се наричат, съответно, *непълно частно* и *остатък* от делението на a с m.

Задача 4. Намерете непълното частно и остатъка от делението на следните числа: а) 56 с 15; б) 91 с 7; в) -42 с 5; г) 0 с 12.

Задача 5. Да се докаже, че ако $a, m \in \mathbb{Z}$ и $m \neq 0$, то съществуват еднозначно определени $q, r \in \mathbb{Z}$, такива че $a = mq + r$ и $0 \leq r < |m|$.

Задача 6. Да се докаже, че ако $a, m \in \mathbb{Z}$ и $m \neq 0$, то съществуват еднозначно определени $q, r \in \mathbb{Z}$, такива че $a = mq + r$ и $-\frac{|m|}{2} < r \leq \frac{|m|}{2}$.

Най–голям общ делител

Определение 3. Нека са дадени числата $a_1, a_2, \ldots, a_n \in \mathbb{Z}$, като поне едно от тях е различно от нула (такава система от цели числа ще наричаме *ненулева*). Едно цяло число се нарича *общ делител* на числата $a_1, a_2, \ldots, a_n$, ако то дели всяко от тях. Най–голямото естествено число, което е общ делител на $a_1, a_2, \ldots, a_n$, се нарича *най–голям общ делител* на $a_1, a_2, \ldots, a_n$ и се означава с $(a_1, a_2, \ldots, a_n)$.

Определение 4. Числата $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ се наричат *взаимно прости*, ако $(a_1, a_2, \ldots, a_n) = 1$. Казваме, че $a_1, a_2, \ldots, a_n$ са *две по две взаимно прости*, ако всеки две тях са взаимно прости.

Пример: Числата 3, 15, 17, 21, 29 са взаимно прости, но не са две по две взаимно прости. Числата 3, 17, 29 са две по две взаимно прости.

Теорема за най–големия общ делител. Най–големият общ d делител на всяка ненулева система от цели числа $a_1, a_2, \ldots, a_n$ може да се представи във вида

$$d = k_1 a_1 + k_2 a_2 + \cdots + k_n a_n \,,$$

където $k_1, k_2, \ldots, k_n \in \mathbb{Z}$ и $(k_1, k_2, \ldots, k_n) = 1$.

В частност, ако $(a_1, a_2, \ldots, a_n) = 1$, то съществуват $k_1, k_2, \ldots, k_n \in \mathbb{Z}$, такива че $d = k_1 a_1 + k_2 a_2 + \cdots + k_n a_n$ и $(k_1, k_2, \ldots, k_n) = 1$.

Задача 7. Да се докаже теоремата за най–големия общ делител.

Решение: Да разгледаме множеството

$$I = \{k_1 a_1 + k_2 a_2 + \ldots k_n a_n \ : \ k_1, k_2, \ldots, k_n \in \mathbb{Z}\} \,.$$

Очевидно $a_i \in I$ за $i = 1, 2, \ldots, n$. Тъй като I съдържа число различно от нула, то I съдържа естествено число. Нека m е най–малкото естествено число, което принадлежи на I (тук използуваме принципа за добрата наредба).

За произволно $a \in I$, съгласно теоремата за деление с частно и остатък, съществуват $q, r \in \mathbb{Z}$, такива че $a = mq + r$ и $0 \leq r < m$. От определението на I следва, че $r = a - mq \in I$ и ако допуснем, че $r \neq 0$, то ще имаме $1 \leq r < m$, което противоречи на избора на m. Тогава $r = 0$ и следователно $m \mid a$. Тъй като $a_i \in I$ за $i = 1, 2, \ldots, n$, то m е общ делител на $a_1, a_2, \ldots, a_n$ и следователно $m \leq d$.

От друга страна, тъй като d е делител на всяко число от I, то $d \mid m$ и тогава $d \leq m$. И така, получаваме, че $d = m$, откъдето следва, че d се представя във вида

$$d = k_1 a_1 + k_2 a_2 + \cdots + k_n a_n \,, \qquad (i)$$

където $k_1, k_2, \ldots, k_n \in \mathbb{Z}$.

Ако положим $l = (k_1, k_2, \ldots, k_n)$, то от (i) следва, че $ld \mid d$, което е възможно само ако $l = 1$.

Задача 8. Да се докаже, че едно число е общ делител на числата от ненулева система точно когато дели техния най–голям общ делител.

Решение: Твърдението следва от определение 3 и от теоремата за най–големия общ делител.

Задача 9. Нека $a, b, c \in \mathbb{Z}$. Да се докаже, че ако $b \mid ac$ и $(a, b) = 1$, то $b \mid c$.

Решение: Понеже $(a, b) = 1$, то според теоремата за най–големия общ делител съществуват $u, v \in \mathbb{Z}$, такива че $au + bv = 1$. Оттук следва, че $acu + bcv = c$. Тъй като по условие $b \mid ac$, то получаваме $b \mid c$.

Задача 10. Да се докаже, че всяко различно от нула рационално число се представя по единствен начин като несъкратима дроб с положителен знаменател.

Упътване: Да се използува задача 9.

Определение 5. Две системи от цели числа наричаме *еквивалентни*, ако едната от тях може да се получи от другата чрез краен брой операции от вида:

а) добавяне или премахване на числа равни на нула,

б) заменяне на число от системата с противоположното му,

в) разместване на две числа в системата,

г) прибавяне към число от системата на цяло число, кратно на друго число от системата.

Задача 11. Да се докаже, че множеството от общи делители на ненулева система от цели числа не се променя, ако тя се замени с еквивалентна на нея система. В частност, не се променя и най–големият общ делител на дадените числа.

Задача 12. Нека са дадени числата $a_1, a_2, \ldots, a_n \in \mathbb{N}$, като е изпълнено $a_1 = \min_{1 \leq k \leq n} a_k$. Нека r_i е остатъкът от делението на a_i с a_1 $(i = 2, 3, \ldots, n)$. Да се докаже, че дадената система е еквивалентна на системата $a_1, r_2, r_3, \ldots, r_n$.

Задача 13. Всяка ненулева система от цели числа е еквивалентна на система, състояща се от едно естествено число, което е равно на най–големия общ делител числата от дадената система.

Упътване: Като използуваме първите три операции от определение 5, премахваме от системата числата равни на нула (ако има такива) и заменяме системата с еквивалентна на нея система от естествени числа, първото от които е минимално. След това заменяме системата с еквивалентната система, описана в задача 12. Чрез повтаряне на този алгоритъм краен брой пъти (тук се използува принципа за добрата наредба) получаваме система, еквивалентна на дадената и състояща се само от едно естествено число. Сега твърдението следва от задача 11.

Забележка: Задача 13 ни дава алгоритъм за изчисляване на най–големия общ делител на произволна ненулева система, състояща се от n на брой цели числа. При $n = 2$ този алгоритъм е известен като *алгоритъм на Евклид.*

Задача 14. Да се намери най–големия общ делител на числата 72, -96, 180, 240, 360, -504.

Решение: Прилагаме алгоритъма от задача 13 и получаваме

$$\begin{aligned}(72,-96,180,240,360,-504) &= (72,96,180,240,360,504) = \\ =(72,24,36,24,0,0) &= (72,24,36,24) = (24,72,36,24) = \\ =(24,0,12,0) &= (24,12) = (12,24) = (12,0) = 12.\end{aligned}$$

Задача 15. Нека $n \geq 2$ и нека числата $a_1, a_2, \ldots, a_n \in \mathbb{N}$ са две по две взаимно прости. Да се докаже, че всяко от тях е взаимно просто с произведението на останалите.

Упътване: При $n = 2$ твърдението е тривиално. Ще го докажем при $n = 3$, а в общия случай то се доказва по индукция. И така, нека $a_1, a_2, a_3 \in \mathbb{N}$ са две по две взаимно прости. Полагаме $d = (a_1, a_2a_3)$. Тогава $d \mid a_1$, $d \mid a_2a_3$ и тъй като $(a_1, a_2) = 1$, то $(d, a_2) = 1$. Тогава според задача 9 имаме $d \mid a_3$ и от условието $(a_1, a_3) = 1$ получаваме, че $d = 1$.

Задача 16. Нека числата $a_1, a_2, \ldots, a_n \in \mathbb{N}$ са две по две взаимно прости и всяко от тях дели числото $k \in \mathbb{N}$. Да се докаже, че произведението $a_1a_2 \ldots a_n$ дели k.

Упътване: Ще докажем твърдението при $n = 2$. В общия случай то се доказва по индукция.

Нека $a_1 \mid k$, $a_2 \mid k$ и $(a_1, a_2) = 1$. Имаме $k = a_1 l$ за някое $l \in \mathbb{N}$. Тъй като $a_2 \mid a_1 l$, то от задача 9 следва, че $a_2 \mid l$. Но тогава $l = a_2 s$ за някое $s \in \mathbb{N}$. В крайна сметка получаваме $k = a_1 a_2 s$, т.е. $a_1 a_2 \mid k$.

Задача 17. Нека $a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_m \in \mathbb{Z}$ и нека $a_1, a_2, \ldots, a_n$ е ненулева система. Да се докаже, че

$$(a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_m) = ((a_1, a_2, \ldots, a_n), b_1, b_2, \ldots, b_m)\,.$$

Упътване: Да се използуват задачи 11 и 13.

Задача 18. Нека $a_1, a_2, \ldots, a_n$ е ненулева система от цели числа и нека $b \in \mathbb{N}$. Да се докаже, че

$$(a_1 b, a_2 b, \ldots, a_n b) = (a_1, a_2, \ldots, a_n) b\,.$$

Решение: Полагаме $(a_1, a_2, \ldots, a_n) = d$ и $(a_1 b, a_2 b, \ldots, a_n b) = h$. Тъй като b е общ делител на $a_1 b, \ldots, a_n b$, то според задача 8) е изпълнено $b \mid h$. По–нататък, $h \mid a_i b$, следователно $\frac{h}{b} \mid a_i$, $i = 1, 2, \ldots, n$. Отново прилагаме задача 8) и получаваме, че $\frac{h}{b} \mid d$, откъдето следва, че $h \mid db$.

От друга страна, имаме $d \mid a_i$. Следователно $db \mid a_i b$, $i = 1, 2, \ldots, n$ и от задача 8) намираме, че $db \mid h$, което ни дава $db = h$.

Задача 19. Нека $a_1, a_2, \ldots, a_n$ и $b_1, b_2, \ldots, b_m$ са две ненулеви системи от цели числа. Да се докаже, че най– големият общ делител на системата числа $a_i b_j$, $1 \leq i \leq n$, $1 \leq j \leq m$ е равен на

$$(a_1, a_2, \ldots, a_n)(b_1, b_2, \ldots, b_m)\,.$$

Упътване: Да разгледаме случая $n = m = 2$ (в общия случай разсъжденията са аналогични). Без ограничение на общността можем да считаме, че $a_1, a_2, b_1, b_2 \in \mathbb{N}$. От задачи 17 и 18 следва, че

$$\begin{aligned}(a_1, a_2)(b_1, b_2) &= (a_1(b_1, b_2), a_2(b_1, b_2)) = ((a_1 b_1, a_1 b_2), (a_2 b_1, a_2 b_2)) \\ &= (a_1 b_1, a_1 b_2, a_2 b_1, a_2 b_2)\,.\end{aligned}$$

Задача 20. Нека числата $a_1, a_2, \ldots, a_n \in \mathbb{N}$ са две по две взаимно прости и нека $b \in \mathbb{N}$. Да се докаже, че

$$(b, a_1 a_2 \ldots a_n) = (b, a_1)\,(b, a_2)\,\ldots(b, a_n)\,.$$

Упътване: Ще докажем твърдението при $n = 2$. В общия случай то се доказва по индукция.

Полагаме $b_i = (b, a_i)$, $i = 1, 2$. Като използуваме задачи 17 и 19 получаваме

$$b_1 b_2 = (b^2, ba_2, ba_1, a_1 a_2) = (b^2, (ba_2, ba_1), a_1 a_2) = (b^2, b(a_2, a_1), a_1 a_2)$$
$$= (b^2, b, a_1 a_2) = (b, a_1 a_2)\,.$$

Задача 21. Нека числата $a_1, a_2, \ldots, a_n \in \mathbb{N}$ са две по две взаимно прости. Да се докаже, че положителните делители на $a_1 a_2 \ldots a_n$ са точно числата $d_1 d_2 \ldots d_n$, където всяко d_i пробягва положителните делители на a_i, $i = 1, 2, \ldots, n$.

Упътване: Ще докажем твърдението при $n = 2$. В общия случай то се доказва по индукция.

Нека $a_1, a_2 \in \mathbb{N}$ и $(a_1, a_2) = 1$. Ако d_1, d_2 са положителни делители съответно на a_1 и a_2, то очевидно имаме $d_1 d_2 \mid a_1 a_2$. Обратно, ако $d \mid a_1 a_2$, $d \in \mathbb{N}$, то от задача 20 следва, че $d = (d, a_1 a_2) = l_1 l_2$, където $l_i = (d, a_i) \mid a_i$, $i = 1, 2$. Числото d се представя еднозначно в посочения вид, тъй като в противен случай ще получим противоречие с резултата от задача 9.

Задача 22. Да се докаже, че числата $F_n = 2^{2^n} + 1$, $n = 1, 2, \ldots$ са две по две взаимно прости.

Упътване: Да се провери, че ако $n, k \in \mathbb{N}$, то е в сила тъждеството

$$F_{n+k} - 2 = F_{n+k-1}\, F_{n+k-2}\, \ldots\, F_{n+1}\, F_n\, (F_n - 2)\,.$$

Забележка: Числата F_n, определени в последната задача, са известни като *числа на Ферма*.

Задача 23. Нека $f(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n$ е полином с цели коефициенти. Да се докаже, че ако несъкратимата рационална дроб $\frac{k}{l}$ е корен на полинома $f(x)$, то $k \mid a_n$ и $l \mid a_0$.

Решение: Можем да считаме, че $a_0 a_n \neq 0$, тъй като в противен случай твърдението е тривиално. От условието $f\left(\frac{k}{l}\right) = 0$ намираме

$$a_0 k^n + a_1 k^{n-1} l + a_2 k^{n-2} l^2 + \cdots + a_{n-1} k l^{n-1} + a_n l^n = 0\,.$$

Оттук следва, че $l \mid a_0 k^n$. Използувайки задача 9 и условието $(k, l) = 1$, получаваме $l \mid a_0$. Имаме също $k \mid a_n l^n$, откъдето $k \mid a_n$.

Задача 24. Да се докаже, че числото $\sqrt{2} + \sqrt[3]{3}$ е ирационално.

Упътване: Да се намери полином с цели коефициенти, който има корен $\sqrt{2} + \sqrt[3]{3}$ и да се приложи задача 23 за да се провери, че този полином няма рационални корени.

Най–малко общо кратно

Определение 6. Нека са дадени числата $a_1, a_2, \ldots, a_n \in \mathbb{Z}$, всяко от които е различно от нула. Едно цяло число се нарича *общо кратно* на числата $a_1, a_2, \ldots, a_n$, ако се дели на всяко от тях. Най–малкото естествено число, което е общо кратно на $a_1, a_2, \ldots, a_n$, се нарича *най–малко общо кратно* на $a_1, a_2, \ldots, a_n$ и се бележи с $[a_1, a_2, \ldots, a_n]$.

Задача 25. Да се докаже, че едно число е общо кратно на няколко числа, точно когато се дели на най–малкото им общо кратно.

Упътване: Да се използува задача 3.

Задача 26. Да се докаже, че най–малкото общо кратно на няколко числа не се променя, ако заменим част от числата с тяхното най–малко общо кратно.

Упътване: Да се използува задача 25.

Задача 27. Нека $a, b \in \mathbb{N}$. Да се докаже, че всяко положително общо кратно на a и b е от вида $\frac{ab}{(a,b)}s$, където $s \in \mathbb{N}$. Като следствие да се изведе формулата $[a, b](a, b) = ab$.

Решение: Нека $k \in \mathbb{N}$ е общо кратно на a и b и нека $(a, b) = d$. Имаме $k = al$ за някое $l \in \mathbb{N}$. Тъй като $b \mid al$, то $\frac{b}{d} \mid \frac{a}{d}l$ и понеже $\left(\frac{b}{d}, \frac{a}{d}\right) = 1$, то от задача 9 получаваме $\frac{b}{d} \mid l$. Тогава $l = \frac{b}{d}s$ за някое $s \in \mathbb{N}$, с което твърдението е доказано.

Следствието е очевидно.

Задача 28. Нека $a, b \in \mathbb{N}$. Да се докажат формулите $([a, b], a) = a$ и $[a, (a, b)] = a$.

Задача 29. Нека $a, b \in \mathbb{N}$. Да се докаже, че следните условия са еквивалентни:

а) $a \mid b$,

б) $[a, b] = b$,

в) $(a, b) = a$.

Задача 30. Нека $a, b, c \in \mathbb{N}$. Да се докажат тъждествата:

а) $([a, b],\, c) = [(a, c),\, (b, c)]$,

б) $[(a, b),\, c] = ([a, c],\, [b, c])$,

в) $([a, b], [b, c], [c, a]) = [(a, b), (b, c), (c, a)]$,

г) $[a, b, c]\,(a, b)\,(b, c)\,(c, a) = (a, b, c)\,a\,b\,c$,

д) $(a, b, c)\,[a, b]\,[b, c]\,[c, a] = [a, b, c]\,a\,b\,c$.

Упътване: Да докажем, например, а). Останалите твърдения се проверяват по подобен начин.

Полагаме $d = ([a, b], c)$, $k = [(a, c), (b, c)]$. Като използуваме задачи 17, 19 и 27, получаваме

$$\begin{aligned} d(a, b)(a, b, c) &= ([a, b](a, b), c(a, b))(a, b, c) = (ab, ac, bc)(a, b, c) \\ &= (a^2b, a^2c, ab^2, ac^2, b^2c, bc^2, abc)\,. \end{aligned}$$

Аналогично

$$\begin{aligned} k(a, b)(a, b, c) &= \frac{(a, c)(b, c)}{((a, c), (b, c))}(a, b)(a, b, c) = (a, c)(b, c)(a, b) \\ &= (ab, bc, ac, c^2)(a, b) = (a^2b, a^2c, ab^2, ac^2, b^2c, bc^2, abc)\,. \end{aligned}$$

Като сравним горните равенства, получаваме $d = k$.

Задача 31. Да се обобщят за произволен брой числа тъждествата г) и д) от задача 30.

Линейни диофантови уравнения

Задача 32. Нека числата $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ образуват ненулева система, $d = (a_1, a_2, \ldots, a_n)$ и нека $b \in \mathbb{Z}$. Да се докаже, че уравнението

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b \qquad (i)$$

има решение $x_1, x_2, \ldots x_n \in \mathbb{Z}$, точно когато $d \mid b$.

Решение: Ако (i) има решение, то d дели лявата му част, следователно $d \mid b$. Нека сега имаме $d \mid b$. Съгласно теоремата за най–големия общ делител съществуват $k_1, k_2, \ldots k_n \in \mathbb{Z}$, такива че $d = a_1k_1 + a_2k_2 + \cdots + a_nk_n$. Тогава числата

$$x_1 = \frac{b}{d}k_1\,, \quad x_2 = \frac{b}{d}k_2\,, \quad \ldots\,, \quad x_n = \frac{b}{d}k_n$$

са цели и удовлетворяват (i).

Забележка: Уравнения, в които се изследва разрешимост в цели числа, се наричат *диофантови уравнения* по името на древногръцкия математик Диофант. Уравнението (i) от задача 32 се нарича линейно диофантово уравнение.

Изследването за разрешимост на диофантови уравнения от вида

$$f(x_1, \ldots, x_n) = 0\,,$$

където f е полином с цели коефициенти, е несравнимо по–сложна задача. Както е показал Матиясевич, не съществува алгоритъм, по който за всеки полином f да може да се определи дали уравнението е разрешимо в цели числа. Все пак, за някои класове от диофантови уравнения задачата за изследване на разрешимостта и намирането на решенията е частично, а в някои случаи, напълно решена.

Задача 33. Да се намери метод за определяне на всички целочислени решения на линейното диофантово уравнение (i) от задача 32 (в случая, когато то е разрешимо).

Упътване: Нека $d = (a_1, a_2, \ldots, a_n)$. Първо игнорираме събираемите от лявата част на уравнението, за които $a_i = 0$. Съответните неизвестни x_i могат да приемат произволни стойности и остава да определим останалите неизвестни. Полагаме

$$c_1 = \min_{\substack{1 \le i \le n \\ a_i \neq 0}} \big(|a_1|, \ldots, |a_n|\big)$$

и нека имаме, например, $c_1 = |a_1|$. Като използуваме задача 5, намираме числа $q_i, r_i \in \mathbb{Z}$, $2 \le i \le n$, такива че

$$a_i = a_1q_i + r_i\,, \quad 0 \le r_i < c_1 \quad \text{при} \quad 2 \le i \le n\,.$$

Полагаме $x_1 = y_1 - \big(q_2x_2 + \cdots + q_nx_n\big)$. Тогава изходното уравнение е еквивалентно на уравнението

$$a_1y_1 + r_2x_2 + \cdots + r_nx_n = b\,,$$

като имаме $d = (a_1, r_2, \ldots, r_n)$. С полученото уравнение работим по същия начин и след краен брой стъпки (тук се използува принципа за добрата наредба на $\mathbb{N}$) стигаме до линейно уравнение, в което някой от коефициентите пред неизвестните е равен на d, а всички останали коефициенти (и също числото b) се делят на d. Съкращаваме на d и изразяваме едно от неизвестните като линейна функция с цели коефициенти на останалите неизвестни, като на тях даваме произволни цели стойности. Връщайки се по обратен ред, намираме неизвестните във вид на линейни функции на няколко променливи, всяка от които пробягва произволни цели стойности.

Забележка: Изложеният алгоритъм за решаване на линейни диофантови уравнения е предложен от Ойлер. Преди да прилагаме метода на Ойлер е разумно да съкратим двете страни на уравнението с $(a_1, a_2, \ldots, a_n)$.

Задача 34. Да се реши в цели числа уравнението

$$90x_1 + 126x_2 + 210x_3 - 315x_4 = 1473\,.$$

Решение: Имаме $(90, 126, 210, 315) = 3$ и $3 \mid 1473$. Съкращаваме на 3 и получаваме еквивалентното уравнение

$$30x_1 + 42x_2 + 70x_3 - 105x_4 = 491\,.$$

Имаме $\min(30, 42, 70, 105) = 30$. В сила са равенствата $42 = 30 \cdot 1 + 12$, $70 = 30 \cdot 2 + 10$, $-105 = 30 \cdot (-4) + 15$. Полагаме $x_1 = y_1 - x_2 - 2x_3 + 4x_4$. Тогава уравнението получава вида

$$30y_1 + 12x_2 + 10x_3 + 15x_4 = 491\,.$$

По–нататък, имаме $\min(30, 12, 10, 15) = 10$ и са изпълнени равенствата $30 = 10 \cdot 3 + 0$, $12 = 10 \cdot 1 + 2$, $15 = 10 \cdot 1 + 5$. Полагаме $x_3 = y_2 - 3y_1 - x_2 - x_4$ и тогава уравнението получава вида

$$2x_2 + 10y_2 + 5x_4 = 491\,.$$

Работейки както преди, намираме $\min(2, 10, 5) = 2$, $10 = 2 \cdot 5 + 0$ и $5 = 2 \cdot 2 + 1$. Полагаме $x_2 = y_3 - 5y_2 - 2x_4$ и уравнението придобива вида $2y_3 + x_4 = 491$. Изразяваме x_4 чрез y_3 и използувайки предидущите равенства, получаваме, че всички решения на даденото уравнение се дават чрез формулите

$$x_1 = 1964 - 7y_3 - 7y_2 + 7y_1\,, \qquad x_2 = -982 + 5y_3 - 5y_2,$$
$$x_3 = 491 - 3y_3 + 6y_2 - 3y_1\,, \qquad x_4 = 491 - 2y_3.$$

където y_1, y_2, y_3 пробягват всевъзможни цели стойности.

Задача 35. Да се решат в цели числа уравненията

а) $6x_1 - 10x_2 + 15x_3 = 1$,

б) $9x_1 + 15x_2 - 21x_3 = 33$,

в) $6x_1 + 15x_2 - 21x_3 + 3x_4 = 55$,

г) $4x_1 + 6x_2 + 8x_3 = 10$,

д) $3x_1 + 4x_2 - 5x_3 = 7$.

Забележка: В следващата задача е описан по–подробно алгоритъм за решаване на линейни диофантови уравнения с две неизвестни.

Задача 36. Нека $a, b, c \in \mathbb{Z}$, $ab \neq 0$, $(a, b) = d$ и нека $d \mid c$.

а) Да се докаже, че ако x_0, y_0 е някакво решение на диофантовото уравнение

$$ax + by = c\,,$$

то всичките му решения са

$$x = x_0 + \frac{b}{d}\,t\,, \quad y = y_0 - \frac{a}{d}\,t\,, \qquad \text{където} \qquad t \in \mathbb{Z}\,.$$

б) Да се даде алгоритъм за намиране на частно решение x_0, y_0.

Упътване: а) От зададените условия лесно се получава равенството $\frac{a}{d}(x - x_0) = -\frac{b}{d}(y - y_0)$. Използуваме, че $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$ и прилагаме задача 9.

б) Можем да считаме, че $b \in \mathbb{N}$. Ако $b = 1$, то $x_0 = 0, y_0 = c$ е решение на уравнението. Да разгледаме случая $b > 1$. Полагаме $r_{-1} = a, r_0 = b$

и прилагайки алгоритъма на Евклид за намиране на (a,b), получаваме системата от равенства

$$\begin{aligned} r_i &= q_{i+2}r_{i+1} + r_{i+2} \quad \text{при} \quad -1 \le i \le s-2\,, \\ r_{s-1} &= q_{s+1}r_s\,, \end{aligned}$$

където $r_i, q_i \in \mathbb{Z}$ и $1 \le r_s < r_{s-1} < \cdots < r_1 < r_0$. По индукция получаваме, че при $1 \le j \le s$ е изпълнено $r_s = P_j r_{s-j-1} + Q_j r_{s-j}$, където P_j, Q_j се определят рекурентно от условията

$$P_1 = 1\,, \quad Q_1 = -q_s\,; \qquad P_{j+1} = Q_j\,, \quad Q_{j+1} = -q_{s-j}Q_j + P_j\,.$$

Ясно е, че $r_s = (r_{-1}, r_0) = (a,b) = d$, следователно $d = P_s a + Q_s b$. Оттук следва, че $x_0 = \frac{c}{d}P_s$, $y_0 = \frac{c}{d}Q_s$ е решение на уравнението.

Задача 37. Да се докаже, че ако $a, b \in \mathbb{N}$ и $(a,b) = d$, то съществуват $a_1, b_1 \in \mathbb{N}$ такива, че $d = aa_1 - bb_1$.

Решение: Твърдението следва от задача 36 а).

Задача 38. Да се решат в цели числа уравненията

а) $1735x + 120y = -25$,

б) $126x - 14y = 81$,

в) $112x - 30y = 46$.

Решение: а) В сила са равенствата

$$1735 = 14 \cdot 120 + 55\,, \quad 120 = 2 \cdot 55 + 10\,, \quad 55 = 5 \cdot 10 + 5\,, \quad 10 = 2 \cdot 5\,,$$

следователно, в означенията от решението на задача 36, имаме $s = 3$; $r_{-1} = 1735$, $r_0 = 120$, $r_1 = 55$, $r_2 = 10$, $r_3 = 5$; $q_1 = 14$, $q_2 = 2$, $q_3 = 5$. Оттук следва, че $(1735, 120) = 5$ и понеже $5 \mid -25$, то уравнението има решение. По–нататък последователно намираме

$$P_1 = 1\,, \quad Q_1 = P_2 = -5\,, \quad Q_2 = P_3 = 11\,, \quad Q_3 = -159\,,$$

откъдето следва, че $x_0 = -55$, $y_0 = 795$ е решение на уравнението. Тогава, според задача 36 а), всичките решения на уравнението се дават чрез формулите

$$x = -55 + 24t\,, \quad y = 795 - 347t\,, \quad \text{където} \quad t \in \mathbb{Z}\,.$$

б) Няма решение.

в) $x = -92 - 15t$, $y = -345 - 56t$, където $t \in \mathbb{Z}$.

2 Прости числа

Разлагане на числата на прости множители

Определение 7. Едно естествено число $n > 1$ се нарича *просто*, ако то няма други естествени делители освен 1 и n. Едно естествено число $n > 1$ се нарича *съставно*, ако то има естествен делител различен от 1 и n. Числото 1 не е нито просто, нито съставно.

Задача 39. Да се докаже, че всяко число $n \in \mathbb{N}$, $n > 1$ притежава прост делител.

Упътване: Да се допусне противното и да се използува принципа за добрата наредба.

Задача 40. Да се докаже, че всяко съставно число $n \in \mathbb{N}$ притежава прост делител, не надминаващ $\sqrt{n}$.

Решение: Според определение 7 числото n се представя във вида $n = km$, където $k, m \in \mathbb{N}$, $1 < k, m < n$. Ако имаме, например, $k \leq m$ и, ако p е прост делител на k, то $n = km \geq k^2 \geq p^2$, с което твърдението е доказано.

Задача 41. а) Да се предложи алгоритъм за намиране на простите числа, които не надминават някое дадено число $x \geq 2$.

б) Да се намерят простите числа, не надминаващи 100.

Упътване: а) От задача 40 следва, че ако числото $n \in \mathbb{N}$ не се дели на просто число, което не надминава $\sqrt{x}$, и ако $\sqrt{x} < n \leq x$, то n е просто. Тогава, ако вече са ни известни простите числа, които не надхвърлят $\sqrt{x}$, то чрез извършване на известен брой деления „отсяваме“ и простите числа, намиращи се в интервала $(\sqrt{x}, x]$. Ако $\sqrt{x}$ е твърде голямо, то прилагаме описаната процедура последователно няколко пъти.

б) 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

Забележка: Горният алгоритъм е известен като *решето на Ератостен* (виж още задача 238). При големи числа x, обаче, описаният алгоритъм практически е неприложим тъй като са необходими извънредно много пресмятания.

Задача 42. Да се намери най–малкото число $n \in \mathbb{N}$, притежаващо свойството: ако p е просто число и $p-1 \mid n$, то $p \mid n$.

Отговор: 1806.

Задача 43. Да се докаже, че за всяко $k \in \mathbb{N}$ съществува $m \in \mathbb{N}$, такова че всички числа $m+1, m+2, \ldots, m+k$ са съставни.

Решение: Можем да изберем $m = (k+1)! - 1$.

Задача 44. Да се докаже, че ако произведение на няколко естествени числа се дели на простото число p, то поне едно от тях се дели на p.

Решение: Достатъчно е да докажем твърдението в случая, когато имаме две числа (в общия случай доказваме по индукция). Нека $a, b \in \mathbb{N}$ и $p \mid ab$. Ако $p \nmid a$, то $(p, a) = 1$ и тогава от задача 9 получаваме, че $p \mid b$.

Задача 45. Нека p е просто число. Да се докаже, че ако $1 \leq k \leq p-1$, то биномният коефициент $\binom{p}{k}$ се дели на p.

Решение: Тъй като $\binom{p}{k} \in \mathbb{N}$, то $k! \mid p(p-1)\ldots(p-k+1)$. Очевидно $(k!, p) = 1$. Тогава от задача 9 имаме $k! \mid (p-1)\ldots(p-k+1)$. Оттук получаваме, че $\binom{p}{k}$ се дели на p.

Основна теорема на аритметиката. Всяко число $n \in \mathbb{N}$, $n > 1$ се разлага на произведение от прости числа и това разлагане е единствено с точност до наредбата на множителите.

Задача 46. Да се докаже основната теорема на аритметиката.

Решение: Първо ще докажем съществуване на разлагането. Допускаме противното. Като използуваме принципа за добрата наредба, можем да считаме, че $n \in \mathbb{N}$, $n > 1$ е най–малкото число, което не може да се представи като произведение на прости множители. Тогава, разбира се, n е съставно число и тогава съществуват $k, m \in \mathbb{N}$, такива че $n = km$ и $1 < k, m < n$. Поради минималния избор на n, всяко от

числата k и m се разлага на произведение от прости числа. Тогава получаваме разлагане и за n, което противоречи на допускането.

Сега ще докажем единствеността на разлагането. Да предположим, че

$$p_1 p_2 \dots p_l = q_1 q_2 \dots q_s \,,$$

където p_i, q_j са прости числа. Понеже p_1 е просто и дели произведението $q_1 q_2 \dots q_s$, то според задача 44 числото p_1 дели някое от числата q_j. Тъй като q_j са прости, то p_1 съвпада с някое от тях. Извършваме съкращение и като разсъждаваме по същия начин получаваме, че p_2 съвпада с някое от числата q_j. Отново съкращаваме и като продължим по същия начин установяваме, че $k = l$ и че всяко от числата p_i съвпада с някое от числата q_j (да забележим, че тук отново използуваме принципа за добрата наредба в $\mathbb{N}$).

Задача 47. Да се докаже единствеността на разлагане на прости множители чрез директно използуване на принципа за добрата наредба и без да се използува задача 44

Решение: Допускаме, че има числа $n \in \mathbb{N}$, $n > 1$, притежаващи две съществено различни разлагания

$$n = p_1 p_2 \dots p_l = q_1 q_2 \dots q_s$$

на прости множители p_i, q_j. Според принципа за добрата наредба може да считаме, че n е най–малкото число с това свойство.

Като използуваме избора на n лесно се установява, че в горното разлагане ще имаме $l > 1$, $s > 1$ и че $p_i \neq q_j$ за всички i, j. В частност, имаме $p_1 \neq q_1$. Без ограничение на общността можем да считаме, че $p_1 < q_1$. Разглеждаме числото $k = (q_1 - p_1) q_2 \dots q_s$, за което е изпълнено $1 < k < n$. Според избора на n, числото k се разлага еднозначно на произведение от прости множители.

От равенството

$$k = q_1 q_2 \dots q_s - p_1 q_2 \dots q_s = p_1 p_2 \dots p_l - p_1 q_2 \dots q_s = p_1 (p_2 \dots p_l - q_2 \dots q_s)$$

следва, че p_1 е прост делител на k. Както вече отбелязахме, k има единствено разлагане на прости множители, следователно или p_1 съвпада с някое от числата $q_2, \dots q_s$, което не е възможно, или пък p_1 ще

дели $q_1 - p_1$, т.е. p_1 ще дели q_1, което също не е възможно. Получаваме противоречие, с което твърдението е доказано.

Забележка: Доказателството, приведено в решението на задача 47, е дадено от Цермело.

Задача 48. Да се реши задача 10 като се използува основната теорема на аритметиката.

Задача 49. Нека $k \in \mathbb{N}$, $k \geq 2$ и нека числото $m \in \mathbb{N}$ не е точна k–та степен. Да се докаже, че числото $\sqrt[k]{m}$ е ирационално.

Упътване: Да се допусне противното и като се използуват задача 10 и основната теорема на аритметиката да се стигне до противоречие.

Забележка: Ирационалността на числото $\sqrt{2}$ е открита още от древните гърци.

Известно е, че числата π и e също са ирационални. Нещо повече, за разлика от $\sqrt{2}$ и $\sqrt{2} + \sqrt[3]{3}$, числата π и e са даже *трансцендентни*, т.е. не са корени на полиноми с цели коефициенти. Трансцендентността на числото e е установена от Ермит, а на π – от Линдеман.

Определение 8. Нека p е просто число. За всяко $n \in \mathbb{N}$ определяме $\mathrm{ord}_p n$ по следния начин. Ако $p \nmid n$ полагаме $\mathrm{ord}_p n = 0$. Ако $p \mid n$, то полагаме $\mathrm{ord}_p n = l$, където $l \in \mathbb{N}$ е най–голямото число, такова че $p^l \mid n$.

Определение 9. *Канонично представяне* на числото $n \in \mathbb{N}$ наричаме

$$n = \prod_p p^{\mathrm{ord}_p n},$$

където произведението е взето по всички прости числа p.

Забележка: В горното произведение има само краен брой множители различни от единица. Съществуването и единствеността на каноничното представяне е осигурено от основната теорема на аритметиката.

Задача 50. Нека числото $n \in \mathbb{N}$, $n > 1$ има канонично представяне $n = p_1^{l_1} p_2^{l_2} \ldots p_s^{l_s}$, където p_i са различни прости числа и $l_i \in \mathbb{N}$. Да се докаже, че положителните делители на n са точно числата $p_1^{\nu_1} p_2^{\nu_2} \ldots p_s^{\nu_s}$, където $\nu_i \in \mathbb{Z}$, $0 \leq \nu_i \leq l_i$, $i = 1, 2, \ldots s$.

Упътване: Да се използува основната теорема на аритметиката.

Задача 51. Нека p е просто число и $n_1,\ n_2 \in \mathbb{N}$. Да се докаже, че $\mathrm{ord}_p(n_1 n_2) = \mathrm{ord}_p n_1 + \mathrm{ord}_p n_2$.

Упътване: Да се използува основната теорема на аритметиката.

Задача 52. Нека $a_1, a_2, \ldots a_n \in \mathbb{N}$ и

$$d = (a_1, a_2, \ldots, a_n), \qquad k = [a_1, a_2, \ldots, a_n].$$

Да се докаже, че за всяко просто число p са в сила равенствата

а) $\mathrm{ord}_p d = \min\left(\mathrm{ord}_p a_1,\ \mathrm{ord}_p a_2,\ \ldots,\ \mathrm{ord}_p a_n\right)$,

б) $\mathrm{ord}_p k = \max\left(\mathrm{ord}_p a_1,\ \mathrm{ord}_p a_2,\ \ldots,\ \mathrm{ord}_p a_n\right)$.

Упътване: Да се използуват основната теорема на аритметиката и определения 3 и 6.

Забележка: Както се вижда от решенията на задачи 46 (в частта за съществуване) и 47, основната теорема на аритметиката може да бъде доказана без да се използува понятието най–голям общ делител. Това ни дава възможност да *дефинираме* числата d и k, определени от равенствата а), съответно б), от задача 52, като най–голям общ делител и, съответно, и най–малко общо кратно на $a_1, \ldots, a_n$.

Задача 53. Да се решат задачи 17 – 30 като се използуват основната теорема на аритметиката и задача 52.

Упътване: Да решим, например, задача 30 д). Нека p е просто число. Да положим $\mathrm{ord}_p a = \alpha$, $\mathrm{ord}_p b = \beta$, $\mathrm{ord}_p c = \gamma$. Без ограничение на общността можем да считаме, че $\alpha \le \beta \le \gamma$. Според задача 52 имаме $\mathrm{ord}_p(a,b,c) = \alpha$, $\mathrm{ord}_p[a,b,c] = \gamma$, $\mathrm{ord}_p[a,b] = \beta$, $\mathrm{ord}_p[a,c] = \gamma$, $\mathrm{ord}_p[b,c] = \gamma$. От тези равенства и от задача 51 виждаме, че p влиза с еднакви степени в каноничните представяния на числата от двете страни на равенството. Остава да приложим основната теорема на аритметиката.

Понятие за p–адични числа

Определение 10. Нека p е просто число. Ще доопределим функцията $\mathrm{ord}_p r$ при $r \in \mathbb{Q}$, $r \neq 0$ по следния начин. Ако $m \in \mathbb{Z}$, $m \neq 0$, то полагаме $\mathrm{ord}_p m = \mathrm{ord}_p |m|$. По–нататък, ако $r \in \mathbb{Q}$, $r \neq 0$ и $r = \frac{m}{n}$, където $m \in \mathbb{Z}$, $m \neq 0$ и $n \in \mathbb{N}$, полагаме $\mathrm{ord}_p r = \mathrm{ord}_p m - \mathrm{ord}_p n$.

Задача 54. Да се докаже, че определението на $\mathrm{ord}_p r$ при $r \in \mathbb{Q}$, $r \neq 0$ е коректно.

Задача 55. Да се докаже, че всяко $r \in \mathbb{Q}$, $r \neq 0$ може да се представи еднозначно във вида

$$r = \varepsilon \prod_p p^{l_p(r)},$$

където произведението е по всички прости числа, $\varepsilon = \pm 1$, $l_p(r) \in \mathbb{Z}$, като $l_p(r) \neq 0$ само за краен брой p. При това имаме $l_p(r) = \mathrm{ord}_p r$.

Упътване: Да се използува основната теорема на аритметиката.

Определение 11. Представянето от задача 55 се нарича *канонично представяне* на числото $r \in \mathbb{Q}$, $r \neq 0$.

Задача 56. Да се намерят каноничните представяния на рационалните числа 60, -168, $\frac{361}{7920}$, $-\frac{175560}{261360}$.

Задача 57. Нека $r, r_1, r_2 \in \mathbb{Q}$, $r r_1 r_2 \neq 0$ и нека $n \in \mathbb{Z}$. Да се докажат равенствата

а) $\mathrm{ord}_p(r_1 r_2) = \mathrm{ord}_p r_1 + \mathrm{ord}_p r_2$,

б) $\mathrm{ord}_p\left(\frac{r_1}{r_2}\right) = \mathrm{ord}_p r_1 - \mathrm{ord}_p r_2$.

в) $\mathrm{ord}_p(r^n) = n \, \mathrm{ord}_p r$.

Определение 12. Нека p е просто число и $r \in \mathbb{Q}$. Определяме *p–адична норма* $||r||_p$ на числото r чрез формулата

$$||r||_p = \begin{cases} p^{-\mathrm{ord}_p r} & \text{ако } r \neq 0\,, \\ 0 & \text{ако } r = 0\,. \end{cases}$$

Задача 58. Нека p е просто число и $r_1, r_2 \in \mathbb{Q}$. Да се докажат следните свойства:

а) $||r_1 r_2||_p = ||r_1||_p \, ||r_2||_p$,

б) $||r_1 + r_2||_p \leq \max\left(||r_1||_p \, , \, ||r_2||_p\right)$,

в) $||r_1||_p < ||r_2||_p \implies ||r_1 + r_2||_p = ||r_2||_p$.

Решение: Доказателството на а) следва директно от задача 57 и определение 12. Да докажем б) и в). Ако някое от числата r_i е равно на нула, разсъжденията са тривиални. В противен случай представяме числата във вида $r_i = p^{l_i} \frac{m_i}{n_i}$, където $l_i = \mathrm{ord}_p r_i$, $m_i \in \mathbb{Z}$, $n_i \in \mathbb{N}$, $p \nmid m_i n_i$; $i = 1, 2$. Можем да считаме, че $l_2 \leq l_1$. Тогава имаме

$$r_1 + r_2 = p^{l_2}\left(p^{l_1 - l_2}\frac{m_1}{n_1} + \frac{m_2}{n_2}\right) = p^{l_2}\frac{m}{n} \, ,$$

където

$$m = p^{l_1 - l_2} m_1 n_2 + m_2 n_1 \, , \qquad n = n_1 n_2 \, .$$

Очевидно $\mathrm{ord}_p n = 0$, $\mathrm{ord}_p m \geq 0$. Тогава $\mathrm{ord}_p(r_1 + r_2) \geq l_2 = \mathrm{ord}_p r_2$ и б) следва от определение 12. Ако пък имаме $l_2 < l_1$, то получаваме даже, че $\mathrm{ord}_p m = \mathrm{ord}_p(m_2 n_1) = 0$. Тогава $\mathrm{ord}_p(r_1 + r_2) = \mathrm{ord}_p r_1$ и в) следва от определение 12.

Задача 59. Нека p е просто число. Определяме p–адично разстояние ρ_p между точките на $\mathbb{Q}$ по следния начин. Ако $r_1, r_2 \in \mathbb{Q}$ полагаме $\rho_p(r_1, r_2) = ||r_1 - r_2||_p$. Да се докаже, че по този начин $\mathbb{Q}$ се превръща в метрично пространство.

Упътване: Да се използува задача 58.

Забележка: Метричните пространсва са са един от основните обекти в математиката. Читателят, който не е запознат с тях, може да се осведоми от всеки по–подробен учебник по математически анализ.

Задача 60. Да се докаже, че в $\mathbb{Q}$ с метриката ρ_2 е изпълнено

$$1 + 2 + 2^2 + 2^3 + \cdots = -1 \, .$$

Решение: Имаме

$$||1+2+2^2+2^3+\cdots+2^n+1||_2 = ||2^{n+1}||_2 = 2^{-n-1} \to 0 \quad \text{когато} \quad n \to \infty \, .$$

Определение 13. Нека p е просто число. Определяме множеството на *p–адичните числа* $\mathbb{Q}_p$ като попълнението на $\mathbb{Q}$ относно метриката от задача 59.

Забележка: Може да се докаже, че ако p е произволно просто число, то алгебричните операции се пренасят по непрекъснатост от $\mathbb{Q}$ в $\mathbb{Q}_p$, така че това метрично пространство е също и поле. При това, пространството $\mathbb{Q}$ с метриката ρ_p от задача 59 не е пълно, т.е. $\mathbb{Q} \neq \mathbb{Q}_p$. Оказва се, че всяко p–адично число се представя във вид на безкраен ред $a_0 + a_1 p + a_2 p^2 + \ldots$, където $a_i \in \mathbb{Z}$, $0 \leq a_i \leq p-1$ за $i = 0, 1, 2, \ldots$ (сходимостта е относно метриката ρ_p).

Полетата $\mathbb{Q}_p$ не са изоморфни на $\mathbb{R}$, нито пък помежду си (при различни p). В $\mathbb{Q}_p$ може да се построи аналог на класическия математически анализ — това е така наречения *p–адичен анализ.* Много от теоремите в тази теория съответстват на теореми от класическия анализ, но има и различия. Например, един ред в $\mathbb{Q}_p$ е сходящ, точно когато общият му член клони към нула. Този факт е следствие от неравенството в свойство б) на задача 58, което е по–силен аналог на неравенството на триъгълника в $\mathbb{R}$.

Полетата на p–адичните числа за математиката са не по–малко важни от полето на реалните числа. Най–важните им приложения са в алгебрата и в теорията на числата. Например, известната теорема на Минковски – Хассе гласи, че една квадратична форма $F(x_1, \ldots, x_n)$ с рационални коефициенти представя нетривиално нулата в $\mathbb{Q}$ (т.е. $F(x_1, \ldots, x_n) = 0$ за някои $x_1, \ldots, x_n \in \mathbb{Q}$, не всички от които са нула), точно когато тази форма представя нетривиално нулата в $\mathbb{R}$ и в $\mathbb{Q}_p$ за всяко просто p.

Полетата $\mathbb{Q}_p$ и p–адичният анализ се прилагат и в други дялове на математиката и дори в математическата физика.

Теорема на Евклид. Съществуват безбройно много прости числа.

Задача 61. Да се докаже теоремата на Евклид.

Решение: Допускаме, че има само краен брой прости числа и нека те са $p_1, p_2, \ldots p_s$. Разглеждаме числото $n = 1 + p_1 p_2 \ldots p_s$. Според задача 39 числото n притежава прост делител p. От нашето допускане следва,

че p съвпада с някое от простите числа p_i, следователно $p \mid p_1 p_2 \dots p_s$, и тогава $p \mid (n-1)$. Оттук правим извода, че $p \mid 1$, което не е възможно, следователно нашето допускане е погрешно.

Забележка: Това е оригиналното доказателство на Евклид.

Задача 62. Да се даде друго доказателство на теоремата на Евклид като се използува задача 22.

Решение: Нека p_n е прост делител на $F_n = 2^{2^n} + 1$. Според задача 22, простите числа p_n, $n = 1, 2, 3 \dots$, са две по две различни, с което твърдението е доказано.

Забележка: Горното доказателство е предложено от Пойа.

Задача 63. Да се докаже, че за всяко $x \in \mathbb{R}$, $x > 2$ е изпълнено неравенството

$$\prod_{p \le x} \left(1 - \frac{1}{p}\right)^{-1} > \sum_{n \le x} \frac{1}{n}.$$

Решение: Да положим $P(x) = \prod_{p \le x} \left(1 - \frac{1}{p}\right)^{-1}$. От формулата за сума от членовете на безкрайна геометрична прогресия получаваме $P(x) = \prod_{p \le x} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \dots\right)$. Като разкрием скобите (тази операция е законна, понеже имаме произведение от краен брой сходящи реда с положителни членове) и като използуваме основната теорема на аритметиката, намираме, че $P(x) = \sum_{n \le x} \frac{1}{n} + \sum'_{n > x} \frac{1}{n}$. В последната формула $\sum'$ означава, че сумирането е взето само по естествени числа, простите делители на които не надминават x. Оттук твърдението следва непосредствено.

Задача 64. Да се докаже теоремата на Евклид като се използува задача 63.

Решение: Като използуваме разходимостта на хармоничния ред получаваме (в означенията на задача 63), че $P(x) \to \infty$, когато $x \to \infty$. Това е възможно само ако съществуват безбройно много прости числа.

Забележка: Последното доказателство на теоремата на Евклид принадлежи на Ойлер. По–внимателен анализ показва нещо повече, а именно, че редът $\sum_p \frac{1}{p}$, където сумирането е разпростряно по всички прости числа, е разходящ. Още по–прецизен резултат е изложен в задача 248.

Определение 14. Казваме, че числото $n \in \mathbb{N}$ е *свободно от квадрати* (или *безквадратно*), ако всеки прост множител в каноничното му разлагане влиза само в първа степен.

Примери: Числата 5, 6 и 10 са безквадратни. Числата 4, 20 и 50 не са безквадратни.

Задача 65. Да се докаже, че всяко число $n \in \mathbb{N}$ се представя еднозначно във вида $n = k^2 q$, където $k, q \in \mathbb{N}$ и q е безквадратно.

Упътване: Доказателството се илюстрира от следния пример:

$$2 \cdot 3^7 \cdot 5^2 \cdot 7^4 \cdot 11^3 = \left(3^3 \cdot 5 \cdot 7^2 \cdot 11\right)^2 \cdot \left(2 \cdot 3 \cdot 11\right).$$

Задача 66. Да се докаже теоремата на Евклид като се използува задача 65.

Решение: Да допуснем, че има краен брой прости числа и нека те са s на брой. Да вземем число $m \in \mathbb{N}$, за което $m > 4^s$, и да разгледаме числата $n \in \mathbb{N}$, $n \leq m$. Очевидно, техният брой е равен на m.

От друга страна, според задача 65, всяко от числата $n \leq m$ се представя еднозначно във вида $n = k^2 q$, където $k, q \in \mathbb{N}$ и q е безквадратно. При това, числата k могат да приемат не повече от $\sqrt{m}$ стойности, а числата q – не повече от 2^s стойности. Следователно числата n са не повече от $\sqrt{m}\, 2^s$.

От горните разсъждения следва, че $m \leq \sqrt{m}\, 2^s$, което противоречи на избора на m.

Забележка: Чрез прецизиране на разсъжденията в решението на задача 66 може да се получи друго доказателство на разходимостта на реда $\sum_p \frac{1}{p}$, където p пробягва всички прости числа.

Задача 67. Казваме, че едно подмножество на $\mathbb{Z}$ е отворено, ако е празното множество или, ако е обединение на множества от вида

$$H_{a,b} = a + b\mathbb{Z} = \{a + kb \ : \ k \in \mathbb{Z}\}$$

където $a, b \in \mathbb{Z}$, $b \neq 0$ (безкрайни в двете посоки аритметични прогресии от цели числа).

а) Да се докаже, че по този начин $\mathbb{Z}$ се превръща в топологично пространство.

б) Да се провери, че всяко множество $H_{a,b}$, където $a, b \in \mathbb{Z}$, $b \neq 0$ е затворено.

Упътване: а) Единственият нетривиален факт, който трябва да се провери е, че сечението на две множества от тип $H_{a,b}$ е или празно или е отново множество от този тип. Доказателството на б) се изяснява от следният пример: $H_{1,4} = \mathbb{Z} \setminus \big(H_{0,4} \cup H_{2,4} \cup H_{3,4}\big)$.

Забележка: Читателят, който не е запознат с понятието „топологично пространство“ и с основните му свойства, може да се осведоми от всеки по–подробен учебник по математически анализ.

Задача 68. Да се използува задача 67 за да се получи друго доказателство на теоремата на Евклид.

Решение: Нека A е обединението от множествата $H_{0,p}$ по всички прости числа p. Очевидно $1 \notin A$, $-1 \notin A$. От друга страна, ако $k \in \mathbb{Z}$, $k \neq \pm 1$, то k притежава прост делител, следователно $k \in A$. Тогава имаме $\mathbb{Z} \setminus A = \{1, -1\}$.

Да допуснем, че има само краен брой прости числа. Тогава множеството A ще бъде затворено, тъй като е обединение на краен брой затворени множества $H_{0,p}$. Следователно множеството $\{1, -1\}$ ще бъде отворено, а това влиза в противоречие с определението на отворено множество в $\mathbb{Z}$.

Забележка: Доказателството на теоремата на Евклид, изложено в решението на задача 68, е предложено от Фюрстенбург.

3 Функциите $[x]$ и $\{x\}$

Определение 15. Нека $x \in \mathbb{R}$. Най–голямото число $n \in \mathbb{Z}$, за което $n \leq x$ се нарича *цяла част на* x (или още *скобка* x) и се бележи с $[x]$. *Дробна част на* x наричаме $\{x\} = x - [x]$.

Примери: $[2,4] = 2$, $[6] = 6$, $[-5,7] = -6$; $\{2,4\} = 0.4$, $\{6\} = 0$, $\{-5,7\} = 0.3$.

Задача 69. Да се провери, че за всяко $x \in \mathbb{R}$ са в сила свойствата:

а) $x - 1 < [x] \leq x$,

б) $0 \leq \{x\} < 1$,

в) $[x] = x \iff x \in \mathbb{Z}$,

г) $[x + a] = [x] + a \iff a \in \mathbb{Z}$,

д) $\{x\} = x \iff 0 \leq x < 1$,

е) $\{x + a\} = \{x\} \iff a \in \mathbb{Z}$.

Задача 70. Да се докаже, че ако $m \in \mathbb{N}$, $a, q, r \in \mathbb{Z}$, като $a = mq + r$ и $0 \leq r < m$, то имаме $q = \left[\frac{a}{m}\right]$, $r = m\left\{\frac{a}{m}\right\}$.

Задача 71. Да се докаже, че ако $x \in \mathbb{R}$ и $n \in \mathbb{N}$, то е изпълнено

$$\sum_{k=0}^{n-1} \left[x + \frac{k}{n}\right] = [nx]\,.$$

Решение: Разглеждаме функцията $h(x) = \sum_{k=0}^{n-1} \left[x + \frac{k}{n}\right] - [nx]$. От определение 15 следва, че ако $0 \leq x < \frac{1}{n}$ то $h(x) = 0$. По–нататък, като използуваме задача 69, установяваме, че $h(x)$ е периодична с период $\frac{1}{n}$. Тогава $h(x) = 0$ за всяко $x \in \mathbb{R}$.

Задача 72. Нека $a, b \in \mathbb{R}$, като $a < b$ и нека $f(x)$ е положителна функция, определена в интервала $[a, b]$. Да се докаже, че броят на точките с целочислени координати, които се намират в криволинейния трапец

$$\{\,(x, y) \in \mathbb{R}^2 \;:\; a < x \leq b\,,\; 0 < y \leq f(x)\,\} \qquad (i)$$

е равен на

$$S = \sum_{a < n \leq b} \big[f(n)\big]\,. \qquad (ii)$$

Упътване: Да се използува определение 15.

Забележка: Класическа задача от теорията на числата е оценяването на броя на целите точки в зададена равнинна област с частично гладка граница. Като разделим областта на части от вида (i), заключаваме, че задачата се свежда до намирането на приближени формули за суми S от вида (ii).

Ясно е, че $S = S_1 - S_2$, където

$$S_1 = \sum_{a<n\leq b} f(n)\,, \qquad S_2 = \sum_{a<n\leq b} \{f(n)\}\,.$$

Сумата S_1 може да бъде изчислена с много добра точност, стига функцията $f(x)$ да е достатъчно гладка (с този въпрос ще се занимаем в § 4). По–нататък, S_2 очевидно удовлетворява $0 \leq S_2 \leq [b] - [a]$. Всичко това ни дава възможност да получим приближена формула за S.

Оказва се, че ако функцията $f(x)$ удовлетворява някои допълнителни условия, то сумата S_2 може да бъде изчислена с много по–добра точност. Ще споменем само, че за тази цел функцията $\{x\}$ се разлага в ред на Фурие по ортогоналната система $e^{2\pi i n x}$, $n = 0, \pm 1, \pm 2 \ldots$, и по този начин изследването на S_2 се свежда до оценяването на експоненциални суми, дефинирани в определение 39 от § 14.

Задача 73. Нека $R \in \mathbb{R}$, $R \geq 1$ и нека $\mathcal{L}(R)$ е броят на точките с целочислени координати, които принадлежат на множеството

$$\{\, (x,y) \in \mathbb{R}^2 \,:\, x > 0\,,\; y > 0\,,\; xy \leq R \,\}\,.$$

Да се докажат тъждествата

а) $$\mathcal{L}(R) = \sum_{n\leq R} \left[\frac{R}{n}\right]\,,$$

б) $$\mathcal{L}(R) = 2 \sum_{n\leq \sqrt{R}} \left[\frac{R}{n}\right] - \left[\sqrt{R}\right]^2\,.$$

Упътване: Равенството а) е директно следствие от задача 72. За доказателството на б) да се използува, че областта, която разглеждаме, е симетрична относно правата $y = x$.

Забележка: При изследване на $\mathcal{L}(R)$ е за предпочитане да използуваме тъждеството б), тъй като сумата, която участвува там, има много по–малко събираеми от сумата в тъждеството а), следователно допускаме по–малка грешка, когато изследваме сумата от дробните части.

Задача 74. Нека $R \in \mathbb{R}$, $R \geq 1$ и нека $\mathcal{K}(R)$ е броят на точките с целочислени координати, които се намират в кръга

$$\{\,(x,y) \in \mathbb{R}^2 \,:\, x^2 + y^2 \leq R\,\}\,.$$

Да се докажат тъждествата

а) $$\mathcal{K}(R) = 4 \sum_{n \leq \sqrt{R}} \left[\sqrt{R - n^2}\right] + 4\left[\sqrt{R}\right] + 1\,,$$

б) $$\mathcal{K}(R) = 8 \sum_{n \leq \sqrt{\frac{R}{2}}} \left[\sqrt{R - n^2}\right] - 4\left[\sqrt{R/2}\right]^2 + 4\left[\sqrt{R}\right] + 1\,.$$

Упътване: Да се използува симетричността на кръга.

Задача 75. Да се докаже, че ако $l, n \in \mathbb{N}$ и $(l,n) = 1$, то е изпълнено

$$\sum_{k=1}^{n-1} \left[\frac{kl}{n}\right] = \frac{1}{2}(l-1)(n-1)\,. \qquad (i)$$

Упътване: Считаме, че $l > 1$ и $n > 1$ (в противен случай твърдението е тривиално). Разглеждаме правоъгълника в равнината с върхове точките $O(0,0)$, $A(0,l)$, $B(n,l)$, $C(n,0)$. Тъй като $(l,n) = 1$, то на диагонала OB няма други целочислени точки, освен краищата му. По–нататък, използуваме задача 72 и установяваме, че сумата от лявата страна на (i) е равна на броя на целочислените точки, които лежат във вътрешността на триъгълника OCB, или все едно, на половината от броя на целочислените точки, които лежат във вътрешността на правоъгълника $OABC$, т.е. на $\frac{1}{2}(l-1)(n-1)$.

Задача 76. Да се докаже, че ако $l, n \in \mathbb{N}$, $2 \nmid nl$ и $(l,n) = 1$, то е изпълнено

$$\sum_{1 \leq k \leq \frac{n-1}{2}} \left[\frac{kl}{n}\right] + \sum_{1 \leq k \leq \frac{l-1}{2}} \left[\frac{kn}{l}\right] = \frac{1}{4}(l-1)(n-1)\,.$$

Упътване: Да се използува метода на решение на задача 75.

Задача 77. Да се докаже, че ако $k \in \mathbb{N}$, $x \in \mathbb{R}$ и $x \geq 0$, то броят на числата $n \in \mathbb{N}$, $n \leq x$, които се делят на k, е точно $\left[\frac{x}{k}\right]$.

Задача 78. Да се докаже, че ако $k \in \mathbb{N}$ и $x \in \mathbb{R}$, то $\left[\frac{x}{k}\right] = \left[\frac{[x]}{k}\right]$.

Упътване: Функцията $\left[\frac{x}{k}\right] - \left[\frac{[x]}{k}\right]$ е периодична по отношение на x с период k и е равна на нула при $0 \leq x < k$.

Задача 79. Да се докаже, че ако $n \in \mathbb{N}$ и p е просто число, то

$$\mathrm{ord}_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \dots .$$

Решение: При $n = 1$ твърдението е очевидно. Нека $n > 1$ и да допуснем, че твърдението е вярно за числата $k \in \mathbb{N}$, $k < n$. Естествените числа, които не надминават n и се делят на p, са p, $2p$, $3p$, $\dots$, tp, където $t = \left[\frac{n}{p}\right]$. Нека v е тяхното произведение и нека u е произведението на естествените числа, не надминаващи n и които не се делят на p. Очевидно имаме $n! = uv$.

Ясно е, че $p \nmid u$, така че $\mathrm{ord}_p u = 0$. По–нататък имаме $v = p^t\, t!$ и, според индукционното предположение, $\mathrm{ord}_p(t!) = \left[\frac{t}{p}\right] + \left[\frac{t}{p^2}\right] + \dots$. Като използуваме задача 51, виждаме, че $\mathrm{ord}_p(n!) = \mathrm{ord}_p v = t + \left[\frac{t}{p}\right] + \left[\frac{t}{p^2}\right] + \dots$. От определението на t и от задача 78 получаваме, че твърдението е вярно и за числото n, с което решението е завършено.

Задача 80. Да се докаже, че за произволни $x_1, x_2, \dots, x_n \in \mathbb{R}$ е изпълнено

$$[x_1] + [x_2] + \dots + [x_n] \leq [x_1 + x_2 + \dots + x_n] .$$

Упътване: Достатъчно е да докажем твърдението при $n = 2$ (в общия случай се доказва по индукция).

Неравенството $[x_1] + [x_2] \leq [x_1 + x_2]$ е еквивалентно на неравенството $\{x_1 + x_2\} \leq \{x_1\} + \{x_2\}$. Тъй като функцията $\{x\}$ е периодична с период 1, то достатъчно е да докажем неравенството при $0 \leq x_1, x_2 < 1$. Остава да се разгледат отделно случаите $x_1 + x_2 < 1$ и $x_1 + x_2 \geq 1$.

Задача 81. Да се докаже, че ако $a_1, a_2, \dots, a_n \in \mathbb{N}$, то

$$\frac{(a_1 + a_2 + \dots + a_n)!}{a_1!\, a_2! \dots a_n!} \in \mathbb{N} .$$

Упътване: Да се приложат задачи 79 и 80 или пък да се използува, че въпросното число е коефициент пред члена $x_1^{a_1} \dots x_n^{a_n}$ в развитието на $(x_1 + \dots + x_n)^{a_1 + \dots + a_n}$.

Задача 82. Да се докаже, че ако $k \in \mathbb{N}$, то произведението на k последователни цели числа се дели на $k!$.

Упътване: Да се приложи задача 81.

Забележка: Последното твърдение следва също от известния факт, че биномните коефициенти са цели числа.

Задача 83. Нека са дадени числата $\alpha, \tau \in \mathbb{R}$, като $\tau \geq 1$. Да се докаже, че съществуват такива $a, q \in \mathbb{Z}$, че

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

Решение: Първо ще намерим такива $k, m \in \mathbb{Z}$, че

$$|\alpha m - k| \leq \frac{1}{\tau}\,, \qquad 1 \leq m \leq \tau\,. \tag{ii}$$

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

$$\{\alpha\}, \{2\alpha\}, \ldots, \{n\alpha\}\,. \tag{iii}$$

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

Да разгледаме накрая случая, когато всички числа (iii) попадат в интервала $\left[\frac{1}{n+1}, \frac{n}{n+1}\right)$. Разделяме го на $n-1$ на брой подинтервала $I_l = \left[\frac{l}{n+1}, \frac{l+1}{n+1}\right)$, $l = 1, 2, \ldots, n-1$ и тъй като числата (iii) са n на брой, то някои две от тях, например $\{s_1\alpha\}$ и $\{s_2\alpha\}$, където $1 \leq s_1 < s_2 \leq n$, попадат в един и същи интервал I_l. Оттук следва, че

$$\left|\{s_2\alpha\} - \{s_1\alpha\}\right| < \frac{1}{n+1}$$

и отново получаваме (ii) при $m = s_2 - s_1$, $k = [s_1\alpha] - [s_2\alpha]$

Като използуваме задача 10, привеждаме дробта $\frac{k}{m}$ към несъкратима дроб $\frac{a}{q}$, като $q \in \mathbb{N}$. Не е трудно да се провери, че числата a и q удовлетворяват (i).

Забележка: При решението на задача 83 бе използуван известният *принцип на Дирихле*. Той гласи, образно казано, че ако в m чекмеджета

се поставят повече от m предмета, то в някое от чекмеджетата ще има повече от един предмет. Този принцип лежи в основата на доказателствата на много теореми от различни области на математиката.

Характерна особеност на принципа на Дирихле е, че с негова помощ се получават *неконструктивни* доказателства за съществуване на обекти от едно или друго естество, без да има алгоритъм, с помощта на който тези обекти да бъдат откривани.

4 Сумационни формули

Определение 16. При $x \in \mathbb{R}$ определяме функцията $\rho_1(x) = \frac{1}{2} - \{x\}$.

Задача 84. Да се провери, че функцията $\rho_1(x)$ притежава свойствата:

а) При $x \in \mathbb{R}$ е изпълнено $-\frac{1}{2} < \rho_1(x) \leq \frac{1}{2}$.

б) При $x \in \mathbb{R} \setminus \mathbb{Z}$ функцията $\rho_1(x)$ е диференцируема и $\rho_1'(x) = -1$.

в) Ако $k \in \mathbb{Z}$, то

$$\lim_{\substack{x \to k \\ x<k}} \rho_1(x) = -\frac{1}{2}\,, \qquad \lim_{\substack{x \to k \\ x \geq k}} \rho_1(x) = \rho_1(k) = \frac{1}{2}\,.$$

г) Функцията $\rho_1(x)$ е периодична с период 1.

Определение 17. За всяко $x \in \mathbb{R}$ определяме функцията

$$\rho_2(x) = \int_0^x \rho_1(t)\,dt\,.$$

Задача 85. Да се провери, че функцията $\rho_2(x)$ притежава свойствата:

а) При $x \in \mathbb{R}$ е изпълнено $0 \leq \rho_2(x) \leq \frac{1}{8}$.

б) Функцията $\rho_2(x)$ е непрекъсната за всяко $x \in \mathbb{R}$ и диференцируема при $x \in \mathbb{R} \setminus \mathbb{Z}$, като в този случай е изпълнено $\rho_2'(x) = \rho_1(x)$.

в) Ако $k \in \mathbb{Z}$, то $\rho_2(k) = 0$.

г) Функцията $\rho_2(x)$ е периодична с период 1.

Задача 86. Нека $a, b \in \mathbb{R}$, $a < b$ и нека $f(x)$ е комплекснозначна непрекъснато диференцируема функция в интервала $[a, b]$. Да се докаже тъждеството

$$\sum_{a<n\leq b} f(n) = \int_a^b f(x)\,dx \,+\, \rho_1(b)f(b) \,-\, \rho_1(a)f(a) \,-\, \int_a^b \rho_1(x)f'(x)\,dx\,.$$

Решение: При $t \in [a, b]$ определяме функциите

$$F(t) = \int_a^t f(x)\,dx - \int_a^t \rho_1(x)f'(x)\,dx\,, \qquad G(t) = \sum_{a<n\leq t} f(n) - \rho_1(t)f(t)\,,$$
$$H(t) = F(t) - G(t)\,.$$

Разглеждаме първо $F(t)$. Тя е непрекъсната в $[a, b]$, а според теоремата на Нютон–Лайбниц е диференцируема при $t \in (a, b)$, като е изпълнено $F'(t) = f(t) - \rho_1(t)f'(t)$.

Сега да разгледаме $G(t)$. Първо ще докажем, че тази функция е непрекъсната в $[a, b]$. Нека $t_0 \in (a, b) \setminus \mathbb{Z}$. Според задача 84, функцията $\rho_1(t)f(t)$ е непрекъсната в t_0, а от друга страна $\sum_{a<n\leq t} f(n)$ не се мени, когато t пробягва малка околност на t_0. Следователно $G(t)$ е непрекъсната в $(a, b) \setminus \mathbb{Z}$. Ако пък $k \in (a, b) \cap \mathbb{Z}$, то от задача 84 и от очевидните равенства

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

получаваме $\lim_{\substack{t\to k\\ t<k}} G(t) = \lim_{\substack{t\to k\\ t\geq k}} G(t) = G(k)$, следователно $G(t)$ е непрекъсната и в точките от $(a, b) \cap \mathbb{Z}$. Аналогично се проверява непрекъснатостта на $G(t)$ в точките a и b. Понеже $F(t)$ и $G(t)$ са непрекъснати в $[a, b]$, то и $H(t)$ е непрекъсната в този интервал.

Нека $k \in \mathbb{Z}$ е такова, че интервалът $I_k = (a, b) \cap (k, k + 1)$ е непразен. Тогава при $t \in I_k$ ще имаме $G'(t) = f(t) - \rho_1(t)f'(t) = F'(t)$. Следователно $H'(t) = 0$ при $t \in I_k$ и $H(t)$ е константа в I_k. Тази константа е една и съща за всяко k понеже $H(t)$ е непрекъсната в $[a, b]$. От всичко това следва, че $H(t)$ е константа в $[a, b]$. Тогава $H(b) = H(a) = \rho_1(a)f(a)$, с което твърдението е доказано.

Задача 87. Да се даде друго доказателство на тъждеството от задача 86.

Упътване: Да се използува равенството

$$\int_a^b \rho_1(x)\, f'(x)\, dx = \sum_{a-1\le n\le b} \int_{(a,b)\cap(n,n+1)} \rho_1(x)\, f'(x)\, dx \; = \\ = \sum_{a-1\le n\le b} \int_{(a,b)\cap(n,n+1)} \Big(\frac{1}{2} + n - x\Big)\, f'(x)\, dx\,,$$

след което да се интегрира по части.

Задача 88. Нека $a, b \in \mathbb{R}$, $a < b$ и нека $f(x)$ е комплекснозначна два пъти непрекъснато диференцируема функция в интервала $[a, b]$. Да се докаже тъждеството

$$\sum_{a<n\le b} f(n) = \int_a^b f(x)\, dx \; + \; \rho_1(b)f(b) \; - \; \rho_1(a)f(a) \; - \\ - \; \rho_2(b)f'(b) \; + \; \rho_2(a)f'(a) \; + \; \int_a^b \rho_2(x)f''(x)\, dx\,.$$

Упътване: Да се работи по някой от методите, изложени в решенията на задачи 86 и 87.

Забележка: Тъждествата от задачи 86 и 88 са известни като *сумационни формули на Ойлер*.

Задача 89. Да се намери обобщение на твърденията от задачи 86 и 88.

Задача 90. Нека $a, b \in \mathbb{R}$, $a < b$ и нека при $n \in \mathbb{N}$, $n \in (a, b]$ са определени числата $c_n \in \mathbb{C}$. Да се докаже, че ако $f(x)$ е комплекснозначна непрекъснато диференцируема функция в интервала $[a, b]$, то е в сила тъждеството

$$\sum_{a<n\le b} c_n\, f(n) = -\int_a^b \Big(\sum_{a<n\le x} c_n\Big)\, f'(x)\, dx \; + \; f(b) \sum_{a<n\le b} c_n\,.$$

Решение: Разглеждаме величината

$$F = f(b) \sum_{a<n\le b} c_n - \sum_{a<n\le b} c_n\, f(n) = \sum_{a<n\le b} c_n \big(f(b) - f(n)\big)\,.$$

От формулата на Нютон–Лайбниц намираме, че

$$F = \sum_{a<n\leq b} c_n \int_n^b f'(x)\,dx = \sum_{a<n\leq b} \int_a^b c_n\, H(x,n)\, f'(x)\,dx\,,$$

където сме положили

$$H(x,n) = \begin{cases} 1 & \text{при } n \leq x \leq b\,, \\ 0 & \text{при } a \leq x < n\,. \end{cases}$$

Като сменим реда на сумирането и интегрирането, получаваме

$$F = \int_a^b \sum_{a<n\leq b} c_n\, H(x,n)\, f'(x)\,dx = \int_a^b \Big(\sum_{a<n\leq x} c_n\Big) f'(x)\,dx\,,$$

което трябваше да се докаже.

Забележка: Тъждеството от задача 90 е известно като *преобразование на Абел*.

Задача 91. Да се докаже, че при $x \in \mathbb{R}$, $x \geq 1$ е в сила асимптотичната формула

$$\sum_{n\leq x} \frac{1}{n} = \ln x + \gamma + \frac{\rho_1(x)}{x} + \mathcal{O}\Big(\frac{1}{x^2}\Big)\,,$$

където γ е константа.

Решение: Използувайки задачи 84, 85 и 88 получаваме

$$\sum_{n\leq x} \frac{1}{n} = 1 + \sum_{1<n\leq x} \frac{1}{n} = 1 + \int_1^x \frac{dt}{t} + \frac{\rho_1(x)}{x} - \frac{1}{2} - \frac{\rho_2(x)}{x^2} + \int_1^x \frac{\rho_2(t)}{t^3}\,dt \;=$$

$$= \ln x + \gamma + \frac{\rho_1(x)}{x} + \Delta(x)\,,$$

където сме положили

$$\gamma = \frac{1}{2} + \int_1^\infty \frac{\rho_2(t)}{t^3}\,dt\,, \qquad \Delta(x) = -\frac{\rho_2(x)}{x^2} - \int_x^\infty \frac{\rho_2(t)}{t^3}\,dt\,.$$

От задача 85 следва, че

$$|\Delta(x)| \leq \frac{|\rho_2(x)|}{x^2} + \int_x^\infty \frac{|\rho_2(t)|}{t^3}\,dt \leq \frac{1}{8x^2} + \frac{1}{8}\int_x^\infty \frac{dt}{t^3} \leq \frac{1}{4x^2}\,.$$

Забележка 1: Константата γ, определена в задача 91, се нарича константа на Ойлер. Известно е, че $\gamma = 0,5772156\ldots$.

Забележка 2: В приложенията най–често се използуват асимптотичната формула

$$\sum_{n\leq x} \frac{1}{n} = \ln x + \gamma + \mathcal{O}\Big(\frac{1}{x}\Big)$$

и оценката

$$\sum_{n\leq x} \frac{1}{n} = \mathcal{O}(\ln x)\,,$$

които се явяват следствия на формулата от задача 91.

Задача 92. Нека $R \in \mathbb{R}$, $R > 1$ и нека величината $\mathcal{L}(R)$ е определена в задача 73.

а) Да се докаже, че

$$\mathcal{L}(R) = R\ln R + (2\gamma - 1) + \Delta(R) + \mathcal{O}(1)\,,$$

където γ е константата на Ойлер и

$$\Delta(R) = 2\sum_{n\leq\sqrt{R}} \rho_1\Big(\frac{R}{n}\Big)\,.$$

б) Да се докаже асимптотичната формула

$$\mathcal{L}(R) = R\ln R + (2\gamma - 1)R + \mathcal{O}\big(\sqrt{R}\big)\,.$$

Упътване: Да се използуват задачи 73 б), 84, 91 и определение 16.

Забележка: Формулата от условие б) е получена от Дирихле. Като се използуват най–простите оценки за експоненциални суми (виж определение 39 от § 14), може да се докаже, че остатъчният член в асимптотичната формула е $\mathcal{O}\big(R^{\frac{1}{3}+\varepsilon}\big)$, където $\varepsilon > 0$ е произволно малко. Същата оценка е получена с елементарни средства от Виноградов. Допълнителни подобрения на показателя се получават чрез по–сложни методи от теорията на експоненциалните суми.

Съществува предположение, според което остатъчният член е даже $\mathcal{O}\big(R^{\frac{1}{4}+\varepsilon}\big)$, където $\varepsilon > 0$ е произволно малко. Тази хипотеза е известна като *проблем за целите точки под хиперболата* и още като *проблем за делителите* (виж задача 263) и все още не е доказана.

Задача 93. Нека $R \in \mathbb{R}$, $R > 1$ и нека величината $\mathcal{K}(R)$ е определена в задача 74.

а) Да се докаже, че

$$\mathcal{K}(R) = \pi R + \Delta'(R) + \mathcal{O}(1)\,,$$

където

$$\Delta'(R) = 8 \sum_{n \le \sqrt{\frac{R}{2}}} \rho_1\big(\sqrt{R - n^2}\,\big)\,.$$

б) Да се докаже асимптотичната формула

$$\mathcal{K}(R) = \pi R + \mathcal{O}\big(\sqrt{R}\,\big)\,.$$

Упътване: Да се използуват задачи 74, 84 и 88.

Забележка: Формулата от условие б) е доказана от Гаус. Както при проблема за делителите и в настоящата асимптотична формула оценката на остатъчния член може да бъде подобрена с помощта на елементарния метод на Виноградов или с методите от теорията на експоненциалните суми. Съществува хипотеза, известна като *проблем за кръга*, според която остатъчният член е $\mathcal{O}\big(R^{\frac{1}{4}+\varepsilon}\big)$, където $\varepsilon > 0$ е произволно малко.

Задача 94. Да се докаже, че при $x \in \mathbb{R}$, $x \ge 2$ е в сила асимптотичната формула

$$\sum_{n \le x} \ln n = x \ln x - x + \mathcal{O}(\ln x)\,.$$

Упътване: Да се приложи задача 86 и да се разсъждава както при решението на задача 91.

Задача 95. Да се докаже, че при $x \in \mathbb{R}$, $x \ge 2$ са в сила следните асимптотични формули и оценки:

а) $$\sum_{n \le x} n^{\alpha} = \frac{x^{\alpha+1}}{\alpha + 1} + \mathcal{O}\big(\max(1, x^{\alpha})\big)\,,$$

където $\alpha \in \mathbb{R}$, $\alpha > -1$, като константата в знака $\mathcal{O}$ зависи от α;

б) $$\sum_{n > x} \frac{1}{n^{\alpha}} = \mathcal{O}\big(x^{1-\alpha}\big)\,,$$

където $\alpha \in \mathbb{R}$, $\alpha > 1$, като константата в знака $\mathcal{O}$ зависи от α;

в) $$\sum_{n \le x} \frac{\ln n}{n} = \frac{1}{2} \ln^2 x + c + \mathcal{O}\Big(\frac{\ln x}{x}\Big)\,,$$

където c е константа.

Задача 96. Да се намерят асимптотични формули за сумите

а) $$\sum_{n \le x} \ln^2 n\,,$$

б) $$\sum_{2 \le n \le x} \frac{1}{\ln n}\,,$$

в) $$\sum_{n \le x} \frac{\sqrt{n}}{1 + \ln n}\,.$$

Задача 97. За всяко $n \in \mathbb{N}$ определяме

$$a_n = \sum_{k=1}^{n} \frac{1}{k\,\ln(n+2-k)}\,.$$

Да се докаже, че редицата a_n, $n = 1, 2, \ldots$ е сходяща и да се намери границата ѝ.

Упътване: Да се раздели дадената сума на две части, като в първата от тях се сумира по числата $k \le \frac{n}{2}$, а във втората — по останалите k.

Отговор: $\lim_{n\to\infty} a_n = 1$.

5 Числови функции – основни свойства

Определение 18. Всяка функция, която е дефинирана в множеството $\mathbb{N}$ и приема стойности в $\mathbb{C}$, се нарича *числова функция*. Някои автори използуват термините *аритметична функция* и *теоретико–числова функция*.

Определение 19. Казваме, че една числова функция $f(n)$ е *мултипликативна*, ако $f(1) = 1$ и, ако при всяка двойка числа n_1, $n_2 \in \mathbb{N}$, такива че $(n_1, n_2) = 1$, е изпълнено $f(n_1 n_2) = f(n_1) f(n_2)$.

Определение 20. Казваме, че една мултипликативна функция $f(n)$ е *напълно мултипликативна*, ако при всяка двойка числа n_1, $n_2 \in \mathbb{N}$ е изпълнено $f(n_1 n_2) = f(n_1) f(n_2)$.

Определение 21. Казваме, че една числова функция $h(n)$ е *адитивна*, ако при всяка двойка числа $n_1, n_2 \in \mathbb{N}$, такива че $(n_1, n_2) = 1$, е изпълнено $h(n_1 n_2) = h(n_1) + h(n_2)$.

Определение 22. Казваме, че една числова функция $h(n)$ е *напълно адитивна*, ако при всяка двойка числа $n_1, n_2 \in \mathbb{N}$ е изпълнено $h(n_1 n_2) = h(n_1) + h(n_2)$.

Задача 98. Да се докаже, че ако числовата функция $h(n)$ е адитивна (напълно адитивна) и ако $a \in \mathbb{C}$, $a \neq 0$ е константа, то функцията $f(n) = a^{h(n)}$ е мултипликативна (напълно мултипликативна).

Забележка: От последната задача се вижда, че в редица случаи изучаването на адитивните функции се свежда до изучаването на мултипликативни функции.

Задача 99. Нека $f(n)$ и $g(n)$ са мултипликативни (напълно мултипликативни) функции.

а) Да се докаже, че функцията $f(n)g(n)$ е мултипликативна (напълно мултипликативна).

б) Да се докаже, че ако $g(n) \neq 0$ за всяко $n \in \mathbb{N}$, то функцията $\frac{f(n)}{g(n)}$ е мултипликативна (напълно мултипликативна).

Задача 100. Да се докаже, че ако функцията $f(n)$ е мултипликативна и ако числото $k \in \mathbb{N}$ има канонично разлагане $k = p_1^{l_1} p_2^{l_2} \dots p_s^{l_s}$, то $f(k) = f\left(p_1^{l_1}\right) f\left(p_2^{l_2}\right) \dots f\left(p_s^{l_s}\right)$.

Задача 101. Да се докаже, че ако $f(n)$ и $g(n)$ са мултипликативни функции, такива че $f\left(p^l\right) = g\left(p^l\right)$ при всяко просто p и при $l \in \mathbb{N}$, то $f(n) = g(n)$ при всяко $n \in \mathbb{N}$.

Задача 102. Да се докаже, че ако $f(n)$ и $g(n)$ са напълно мултипликативни функции и $f(p) = g(p)$ за всяко просто p, то $f(n) = g(n)$ за всяко $n \in \mathbb{N}$.

Определение 23. Нека е дадена числовата функция $f(n)$. Функцията

$$F(n) = \sum_{d|n} f(d)$$

(сумата е по положителните делители d на n) се нарича *функция сума* за $f(n)$.

Задача 103. Да се докаже, че за всяка числова функция $F(n)$ съществува една единствена числова функция $f(n)$, чиято функция сума е $F(n)$.

Решение: Съществуване: Ще определим числовата функция $f(n)$ индуктивно. Полагаме $f(1) = F(1)$. Да допуснем, че $n > 1$ и нека сме определили $f(k)$ при всички естествени числа $k < n$. Тогава определяме

$$f(n) = F(n) - \sum_{\substack{k|n \\ k<n}} f(k)\,.$$

Очевидно е, че функцията $F(n)$ е функция сума за така определената числова функция $f(n)$.

Единственост: Да допуснем, че има две числови функции $f(n)$ и $f_1(n)$, такива че при всяко $n \in \mathbb{N}$ е изпълнено

$$F(n) = \sum_{d|n} f(d) = \sum_{d|n} f_1(d)\,. \qquad (i)$$

Очевидно имаме $f(1) = f_1(1) = F(1)$. Нека $n \in \mathbb{N}$, $n > 1$ и нека допуснем, че за всяко $k \in \mathbb{N}$, за което $k < n$, е изпълнено $f(k) = f_1(k)$. Тогава от (i) намираме, че

$$f(n) = F(n) - \sum_{\substack{d|n \\ d<n}} f(d) = F(n) - \sum_{\substack{d|n \\ d<n}} f_1(d) = f_1(n)\,.$$

От принципа на математическата индукция следва, че $f(n) = f_1(n)$ за всяко $n \in \mathbb{N}$.

Забележка: Последната задача ни дава възможност при дадена функция $F(n)$ да *дефинираме* числовата функция $f(n)$ чрез равенството от определение 23. Явна формула за изразяване на $f(n)$ чрез $F(n)$ е дадена в задача 113.

Задача 104. Да се докаже, че ако функцията $f(n)$ е мултипликативна, то такава е също и нейната функция сума $F(n)$.

Решение: Нека $n_1, n_2 \in \mathbb{N}$ и $(n_1, n_2) = 1$. Като използуваме задача 21, получаваме

$$F(n_1 n_2) = \sum_{d \mid n_1 n_2} f(d) = \sum_{d_1 \mid n_1} \sum_{d_2 \mid n_2} f(d_1 d_2) =$$
$$= \sum_{d_1 \mid n_1} \sum_{d_2 \mid n_2} f(d_1) f(d_2) = \sum_{d_1 \mid n_1} f(d_1) \sum_{d_2 \mid n_2} f(d_2) = F(n_1) F(n_2) .$$

Задача 105. Да се докаже, че ако $F(n)$ е функция сума за $f(n)$ и ако $F(n)$ е мултипликативна, то $f(n)$ също е мултипликативна.

Решение: От равенството $F(n) = \sum_{d \mid n} f(d)$ и от условието за мултипликативност на $F(n)$ следва, че $f(1) = F(1) = 1$.

Да допуснем, че $f(n)$ не е мултипликативна. Тогава съществуват $n_1, n_2 \in \mathbb{N}$, такива че $(n_1, n_2) = 1$ и $f(n_1 n_2) \neq f(n_1) f(n_2)$. Избираме такива n_1, n_2 с минимално произведение (това е възможно поради принципа за добрата наредба в $\mathbb{N}$). За така избраните n_1, n_2 очевидно имаме $n_1 > 1$, $n_2 > 1$.

Като използуваме условието, че $F(n)$ е функция сума на $f(n)$, задача 21 и избора на n_1, n_2, получаваме

$$F(n_1 n_2) = \sum_{d \mid n_1 n_2} f(d) = f(n_1 n_2) + \sum_{\substack{d \mid n_1 n_2 \\ d < n_1 n_2}} f(d) =$$
$$= f(n_1 n_2) + \sum_{\substack{d_1 \mid n_1 \\ d_1 d_2 < n_1 n_2}} \sum_{d_2 \mid n_2} f(d_1 d_2) =$$
$$= f(n_1 n_2) + \sum_{\substack{d_1 \mid n_1 \\ d_1 d_2 < n_1 n_2}} \sum_{d_2 \mid n_2} f(d_1) f(d_2) .$$

От друга страна имаме

$$F(n_1)F(n_2) = \sum_{d_1|n_1} f(d_1) \sum_{d_2|n_2} f(d_2) = \sum_{d_1|n_1} \sum_{d_2|n_2} f(d_1)f(d_2) =$$
$$= f(n_1)f(n_2) + \sum_{\substack{d_1|n_1 \\ d_1 d_2 < n_1 n_2}} \sum_{d_2|n_2} f(d_1)f(d_2)\,.$$

Най–накрая, поради условието за мултипликативност на $F(n)$, имаме $F(n_1n_2) = F(n_1)F(n_2)$. От последните три равенства получаваме, че $f(n_1n_2) = f(n_1)f(n_2)$, което е в противоречие с избора на n_1 и n_2. Следователно нашето допускане не е вярно и функцията $f(n)$ е мултипликативна.

Задача 106. Нека $f(n)$ е мултипликативна функция и $F(n)$ е нейната функция сума. Да се докаже, че ако числото $k \in \mathbb{N}$, $k > 1$ има канонично разлагане $k = p_1^{l_1} p_2^{l_2} \ldots p_s^{l_s}$, то

$$F(k) = \prod_{i=1}^{s} \left(1 + f\left(p_i\right) + f\left(p_i^2\right) + \cdots + f\left(p_i^{l_i}\right)\right).$$

Упътване: Когато k е степен на просто число твърдението е очевидно. В общия случай да се използува мултипликативността на $F(n)$.

Задача 107. Нека $f(n)$ е мултипликативна функция. Да се докаже, че за произволни $n_1, n_2 \in \mathbb{N}$ е в сила равенството

$$f\left([n_1, n_2]\right) f\left((n_1, n_2)\right) \;=\; f(n_1)\, f(n_2)\,.$$

Упътване: Да се използуват задачи 52 и 100.

Задача 108. Нека $f(n)$ е мултипликативна функция и нека безкрайният ред $\sum_{n=1}^{\infty} f(n)$ е абсолютно сходящ. Да се докаже, че е в сила тъждеството

$$\sum_{n=1}^{\infty} f(n) = \prod_{p} \left(1 + f(p) + f(p^2) + f(p^3) + \ldots\right), \qquad (i)$$

където произведението е взето по всички прости числа.

Ако освен това функцията $f(n)$ е напълно мултипликативна, то е изпълнено

$$\sum_{n=1}^{\infty} f(n) = \prod_{p} \big(1 - f(p)\big)^{-1} . \qquad (ii)$$

Решение: Нека за всяко просто число p положим

$$\gamma_p = 1 + f(p) + f(p^2) + f(p^3) + \dots .$$

Да отбележим, че редът, който определя γ_p, е абсолютно сходящ поради абсолютната сходимост на $\sum_{n=1}^{\infty} f(n)$.

При всяко $x \in \mathbb{R}$, $x > 2$ разглеждаме величината $P(x) = \prod_{p \le x} \gamma_p$. Умножаваме тези краен брой абсолютно сходящи редове и използуваме основната теорема на аритметиката и мултипликативността на $f(n)$. Получаваме

$$P(x) = \sum_{n \le x} f(n) + \Delta(x) , \qquad (iii)$$

където $\Delta(x) = \sum'_{n>x} f(n)$, като $\sum'$ означава, че сумирането се извършва по числа, простите делители на които не надхвърлят x.

Очевидно имаме $|\Delta(x)| \le \sum_{n>x} |f(n)|$, следователно

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

Като извършим граничен преход в (iii), получаваме (i).

Ако функцията $f(n)$ е напълно мултипликативна, то за всяко просто число p имаме $f(p) \neq 1$, тъй като в противен случай редът, който представлява γ_p, би бил разходящ, а това противоречи на условието. За да докажем (ii) остава да забележим, че $\gamma_p = \big(1 - f(p)\big)^{-1}$ и да приложим тъждеството (i).

Забележка: Формулата (i) е известна като *тъждество на Ойлер* .

6 Някои по–важни числови функции

Определение 24. Нека $n \in \mathbb{N}$. Означаваме с $\omega(n)$ броят на различните прости делители на n, а с $\Omega(n)$ – броят на всички прости множители в каноничното разлагане на n.

Примери: Имаме $\omega(6) = \Omega(6) = 2$, $\omega(8) = 1$, $\Omega(8) = 3$.

Задача 109. Да се провери, че функцията $\omega(n)$ е адитивна, а функцията $\Omega(n)$ – напълно адитивна.

Определение 25. Определяме *функцията на Мьобиус* $\mu(n)$ чрез равенството

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

Задача 110. Да се докаже, че функцията на Мьобиус е мултипликативна.

Решение: Използуваме задача 105 и тривиалния факт, че функцията от дясната страна на равенството от определение 25 е мултипликативна.

Задача 111. Да се докаже, че функцията на Мьобиус удовлетворява условията

а) $\mu(1) = 1$,

б) $\mu(n) = 0$ ако $p^2 \mid n$ за някое просто число p.

в) $\mu(n) = (-1)^s$ ако n е произведение на s различни прости числа.

Решение: Равенството $\mu(1) = 1$ следва директно от определението на функцията на Мьобиус.

Тъй като според задача 110 функцията $\mu(n)$ е мултипликативна, то за доказателството на свойствата б) и в) е достатъчно да проверим, че ако p е просто число, то $\mu(p) = -1$ и че $\mu(p^l) = 0$ при $l \in \mathbb{N}$, $l > 1$.

Имаме

$$0 = \sum_{d|p} \mu(d) = \mu(1) + \mu(p) = 1 + \mu(p)\,,$$

следователно $\mu(p) = -1$.

По–нататък, при $l = 2$ е изпълнено

$$0 = \sum_{d|p^2} \mu(d) = \mu(1) + \mu(p) + \mu(p^2) = 1 - 1 + \mu(p^2) = \mu(p^2)\,.$$

Ако $l \geq 3$ и ако сме доказали, че $\mu(p^s) = 0$ за числата $s \in \mathbb{N}$, такива че $2 \leq s \leq l-1$, то имаме

$$0 = \sum_{d|p^l} \mu(d) = \mu(1) + \mu(p) + \cdots + \mu(p^l) = 1 - 1 + 0 + \cdots + 0 + \mu(p^l) = \mu(p^l)\,.$$

Тогава по принципа на математическата индукция заключаваме, че $\mu(p^l) = 0$ при всяко $l \in \mathbb{N}$, $l \geq 2$, с което решението на задачата е завършено.

Задача 112. Нека сме определили функцията $\mu(n)$ чрез условията а), б) и в) от задача 111. Да се изведе като следствие формулата от определение 25.

Задача 113. Нека са дадени числовите функции $F(n)$ и $f(n)$. Да се докаже, че следните твърдения са еквивалентни:

а) Функцията $F(n)$ е функция сума за $f(n)$.

б) За всяко $n \in \mathbb{N}$ е изпълнено

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

Решение: Нека е изпълнено а), т.е. при $n \in \mathbb{N}$ е в сила $F(n) = \sum_{d|n} f(d)$. За всяко $n \in \mathbb{N}$ определяме

$$\Phi(n) = \sum_{d|n} \mu(d)\, F\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \sum_{t|\frac{n}{d}} f(t)\,.$$

Като сменим реда на сумирането и използуваме определение 25, получаваме

$$\Phi(n) = \sum_{t|n} f(t) \sum_{d|\frac{n}{t}} \mu(d) = f(n)\,,$$

с което твърдение б) е доказано.

Аналогично се проверява, че от б) следва а).

Задача 114. Нека $F(x)$ и $f(x)$ са функции, дефинирани при $x \in \mathbb{R}$, $x > 0$ и тъждествено равни на нула при достатъчно големи x. Да се докаже, че следните две твърдения са еквивалентни:

а) За всяко $x > 0$ е изпълнено

$$F(x) = \sum_{k=1}^{\infty} f(kx)\,.$$

б) За всяко $x > 0$ е изпълнено

$$f(x) = \sum_{k=1}^{\infty} \mu(k)\, F(kx)\,.$$

Решение: Нека е изпълнено а). За всяко $x > 0$ определяме

$$H(x) = \sum_{k=1}^{\infty} \mu(k)\, F(kx) = \sum_{k=1}^{\infty} \mu(k) \sum_{l=1}^{\infty} f(lkx)\,.$$

Като пренаредим събираемите и използуваме определение 25, получаваме

$$H(x) = \sum_{m=1}^{\infty} \sum_{\substack{k=1 \\ kl=m}}^{\infty} \sum_{l=1}^{\infty} \mu(k)\, f(lkx) = \sum_{m=1}^{\infty} f(mx) \sum_{k|m} \mu(k) = f(x)\,,$$

с което б) е доказано. Аналогично получаваме, че от б) следва а).

Задача 115. Нека $F(x)$ и $f(x)$ са функции, дефинирани за $x \in \mathbb{R}, x > 0$. Да се докаже, че следните две твърдения са еквивалентни:

а) За всяко $x > 0$ е изпълнено

$$F(x) = \sum_{k \le x} f\left(\frac{x}{k}\right)\,.$$

б) За всяко $x > 0$ е изпълнено

$$f(x) = \sum_{k \le x} \mu(k)\, F\left(\frac{x}{k}\right)\,.$$

Упътване: Да се работи както при решението на задачи 113 и 114.

Забележка: Твърденията от задачи 113 – 115 са известни под името *формули на Мьобиус за обръщане*.

Задача 116. Да се докаже, че при всяко $x \in \mathbb{R}$, $x \geq 1$ е изпълнено

$$1 = \sum_{k \leq x} \mu(k) \left[\frac{x}{k}\right].$$

Упътване: Да се приложи задача 115 за функцията $f(x)$, дефинирана като $f(x) = 1$ при всяко $x > 0$.

Задача 117. Да се докаже, че ако $k, n \in \mathbb{N}$, то е в сила тъждеството

$$\sum_{d^k \mid n} \mu(d) = \begin{cases} 0 & \text{ако за някое просто } p \text{ имаме } p^k \mid n, \\ 1 & \text{в противен случай} \end{cases}$$

(сумата е по всички $d \in \mathbb{N}$, такива че $d^k \mid n$).

Упътване: Първо да се установи, че функциите от двете страни на равенството са мултипликативни. След това да се провери, че тъждеството е вярно при $n = p^l$, където p е просто и $l \in \mathbb{N}$ и да се използува задача 101.

Определение 26. За всяко $n \in \mathbb{N}$ определяме *функцията на Лиувил* $\lambda(n)$ чрез равенството

$$\sum_{d \mid n} \lambda(d) = \begin{cases} 1 & \text{ако } n \text{ е точен квадрат}, \\ 0 & \text{в противен случай.} \end{cases}$$

Задача 118. Да се докаже, че функцията на Лиувил е мултипликативна.

Упътване: Да се използува задача 105.

Задача 119. Да се докаже, че при $n \in \mathbb{N}$ е изпълнено $\lambda(n) = (-1)^{\Omega(n)}$.

Упътване: От задача 101 следва, че е достатъчно равенството да се установи при $n = p^l$, където p е просто и $l \in \mathbb{N}$. В този случай твърдението се доказва чрез индукция по l като се използува определение 26.

Задача 120. Да се докаже, че при всяко $x \in \mathbb{R}$, $x \geq 1$ е изпълнено

$$[\sqrt{x}] = \sum_{k \leq x} \lambda(k) \left[\frac{x}{k}\right].$$

Упътване: Да се използуват задача 77 и определение 26.

Определение 27. При $n \in \mathbb{N}$ определяме *функцията на Манголд* $\Lambda(n)$ посредством равенството

$$\sum_{d|n} \Lambda(d) = \ln n \,.$$

Задача 121. Да се докаже, че при всяко $n \in \mathbb{N}$ е изпълнено

$$\Lambda(n) = \sum_{d|n} \mu(d)\, \ln \frac{n}{d} = -\sum_{d|n} \mu(d)\, \ln d \,.$$

Упътване: Да се използуват задача 113 и определения 25 и 27.

Задача 122. Да се докаже, че ако числата $n_1, n_2 \in \mathbb{N}$ удовлетворяват $n_1, n_2 > 1$ и $(n_1, n_2) = 1$, то е изпълнено $\Lambda(n_1 n_2) = 0$.

Решение: Като използуваме задачи 21 и 121, получаваме

$$\begin{aligned}
\Lambda(n_1 n_2) &= -\sum_{d|n_1 n_2} \mu(d)\, \ln d = -\sum_{d_1|n_1} \sum_{d_2|n_2} \mu(d_1)\, \mu(d_2)\, \ln(d_1 d_2) = \\
&= -\sum_{d_1|n_1} \sum_{d_2|n_2} \mu(d_1)\, \mu(d_2)\, (\ln d_1 + \ln d_2) = \\
&= -\sum_{d_1|n_1} \mu(d_1)\, \ln d_1 \sum_{d_2|n_2} \mu(d_2) - \sum_{d_2|n_2} \mu(d_2)\, \ln d_2 \sum_{d_1|n_1} \mu(d_1) \,.
\end{aligned}$$

Вътрешните суми в горното равенство са равни на нула според определение 25, с което твърдението е доказано.

Задача 123. Да се докаже, че за всяко $n \in \mathbb{N}$ е изпълнено

$$\Lambda(n) = \begin{cases} \ln p & \text{ако } n = p^l \,, \text{ където } p \text{ е просто и } l \in \mathbb{N} \,, \\ 0 & \text{в противен случай} \,. \end{cases}$$

Решение: От задача 121 следва, че $\Lambda(1) = 0$. Да разгледаме случая $n > 1$. Ако n притежава поне два различни прости делителя p_1 и p_2, то n може да се представи във вида $n = p_1^{l_1} p_2^{l_2} m$, където $l_1, l_2, m \in \mathbb{N}$ и $(p_1 p_2, m) = 1$. Като приложим задача 122 с $n_1 = p_1^{l_1}$, $n_2 = p_2^{l_2} m$, получаваме $\Lambda(n) = 0$.

Остана да разгледаме случая, когато $n = p^l$ при просто p и при $l \in \mathbb{N}$. Като използуваме задачи 50, 111 и 121, получаваме

$$\Lambda\left(p^l\right) = -\sum_{d|p^l} \mu(d)\, \ln d = -\sum_{\nu=0}^{l} \mu\left(p^\nu\right)\, \ln p^\nu = \ln p\,.$$

Задача 124. Нека сме определили $\Lambda(n)$ чрез формулата от задача 123. Да се изведе като следствие формулата от определение 27.

Задача 125. Да се докаже, че при $x \in \mathbb{R}$, $x \geq 2$ е в сила асимптотичната формула

$$\sum_{k \leq x} \Lambda(k) \left[\frac{x}{k}\right] = x \ln x - x + \mathcal{O}(\ln x)\,.$$

Решение: Като използуваме задачи 77, 94 и определение 27, получаваме

$$\sum_{k \leq x} \Lambda(k) \left[\frac{x}{k}\right] = \sum_{k \leq x} \Lambda(k) \sum_{\substack{n \leq x \\ k \mid n}} 1 = \sum_{n \leq x} \sum_{k|n} \Lambda(k) =$$

$$= \sum_{n \leq x} \ln n = x \ln x - x + \mathcal{O}(\ln x)\,.$$

Определение 28. При $n \in \mathbb{N}$ определяме *функцията на Ойлер* $\varphi(n)$ като броя на числата $k \in \mathbb{N}$, $k \leq n$, такива че $(k, n) = 1$. Числото $\varphi(n)$ се нарича още *индикатор* на n.

Задача 126. Да се докаже формулата

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

Решение: Като използуваме задача 8) и определения 25, 28, получаваме

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

Сега сменяме реда на сумирането и намираме, че

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

Сумата по k е точно равна на $\frac{n}{d}$, с което твърдението е доказано.

Задача 127. Да се докаже, че при всяко $n \in \mathbb{N}$ е в сила тъждеството

$$n = \sum_{d|n} \varphi(d)\,.$$

Решение: Твърдението следва от задачи 113 и 126.

Задача 128. Да се даде директно доказателство на тъждеството от задача 127.

Решение: Разглеждаме дробите $\frac{1}{n}, \frac{2}{n}, \frac{3}{n}, \ldots, \frac{n-1}{n}, \frac{n}{n}$ и представяме всяка от тях като положителна несъкратима дроб. Получените знаменатели ще бъдат всевъзможните делители на n. При това, ако $d \mid n$ и $d > 0$, то точно $\varphi(d)$ от получените дроби ще имат знаменател d.

Задача 129. Да се докаже, че функцията на Ойлер е мултипликативна.

Решение: Следва от задачи 104, 126 и от мултипликативността на функцията $\frac{\mu(n)}{n}$, или пък от задачи 104 и 127.

Задача 130. Да се докаже, че функцията на Ойлер удовлетворява

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

Решение: Твърдението следва от задачи 106, 111 и 126.

Задача 131. Като се използува задача 130 да се даде ново доказателство на теоремата на Евклид за съществуването на безбройно много прости числа.

Решение: Да допуснем, че има краен брой прости числа и те са $p_1 = 2,\ p_2 = 3, \ldots, p_s$. Полагаме $n = p_1 p_2 \ldots p_s$ и разглеждаме числото $m = \varphi(n)$. Имаме $m = 1$, тъй като числото $k = 1$ е взаимно просто с n и всяко цяло $k \geq 2$ се дели на някое от числата $p_1, p_2, \ldots, p_s$ поради допускането, че това са всички прости числа. От друга страна, от задача 130 получаваме $m = \prod_{i=1}^{s}(p_i - 1) > 1$. От полученото противоречие следва, че нашето допускане е погрешно, т.е. съществуват безбройно много прости числа.

Задача 132. Да се докаже, че за всяко $n \in \mathbb{N}$ е изпълнено

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

Решение: От задачи 99, 110 и 129 следва, че числовата функция $\frac{\mu^2(n)}{\varphi(n)}$ е мултипликативна. Като приложим задача 104 получаваме, че е мултипликативна и нейната функция сума. От друга страна, числовата функция $\frac{n}{\varphi(n)}$ също е мултипликативна. Следователно, според задача 101, за да докажем тъждеството е достатъчно да го проверим при $n = p^l$, където p е просто и $l \in \mathbb{N}$. При такова n, като използуваме задача 130, получаваме

$$\frac{n}{\varphi(n)} = \frac{n}{n\left(1 - \frac{1}{p}\right)} = \frac{p}{p-1} .$$

От друга страна, от задачи 50, 111 и 130 следва, че

$$\sum_{d|n} \frac{\mu^2(d)}{\varphi(d)} = \sum_{\nu=0}^{l} \frac{\mu^2\left(p^\nu\right)}{\varphi\left(p^\nu\right)} = 1 + \frac{\mu^2(p)}{\varphi(p)} = 1 + \frac{1}{p-1} = \frac{p}{p-1} ,$$

с което задачата е решена.

Определение 29. Определяме функцията $\tau(n) = \sum_{d|n} 1$ – броя на делителите на числото $n \in \mathbb{N}$.

Задача 133. Да се докаже, че функцията $\tau(n)$ е мултипликативна.

Решение: Твърдението следва непосредствено от задача 104 и от определение 29.

Задача 134. Да се докаже, че ако числото $n \in \mathbb{N}$, $n > 1$, има канонично разлагане $n = p_1^{l_1} p_2^{l_2} \dots p_s^{l_s}$, то $\tau(n) = (l_1 + 1)(l_2 + 1) \dots (l_s + 1)$.

Решение: Следва от задача 106 или пък от задача 50.

Задача 135. Да се докаже, че за всички $n_1, n_2 \in \mathbb{N}$ е изпълнено

$$\tau(n_1 n_2) \leq \tau(n_1)\, \tau(n_2) .$$

Упътване: Да се използува задача 134.

Задача 136. Да се докаже, че за всяко $n \in \mathbb{N}$ е в сила тъждеството

$$\sum_{d|n} \tau^3(d) = \Big(\sum_{d|n} \tau(d) \Big)^2 .$$

Упътване: Да се използуват задачи 101, 104, 133 и елементарното тъждество $\sum_{k=1}^{m} k^3 = \big(\sum_{k=1}^{m} k \big)^2$.

Задача 137. Да се докаже, че за всяко $\varepsilon \in \mathbb{R}$, $\varepsilon > 0$ съществува константа $C(\varepsilon) > 0$, такава че за всяко $n \in \mathbb{N}$ е в сила неравенството

$$\tau(n) \leq C(\varepsilon)\, n^{\varepsilon} .$$

Решение: При $\varepsilon \geq 1$ твърдението следва от тривиалното неравенство $\tau(n) \leq n$, така че остава да разгледаме случая $0 < \varepsilon < 1$. Можем да считаме, че $n > 1$. Нека каноничното му разлагане е $n = p_1^{l_1} p_2^{l_2} \ldots p_s^{l_s}$, където $l_i \in \mathbb{N}$. Имаме

$$\frac{\tau(n)}{n^{\varepsilon}} = \prod_{i=1}^{s} \frac{l_i + 1}{p_i^{\varepsilon l_i}} = U\, V ,$$

където U е произведението, взето по индексите i, такива че $p_i \leq 2^{1/\varepsilon}$, а V е произведението по останалите i.

Да разгледаме V. Тъй като при всяко $l \in \mathbb{N}$ е изпълнено $2^l \geq l + 1$, то при $p_i > 2^{1/\varepsilon}$ имаме

$$\frac{l_i + 1}{p_i^{\varepsilon l_i}} \leq \frac{l_i + 1}{2^{l_i}} \leq 1 ,$$

следователно $V \leq 1$.

По–нататък, U е произведение на не–повече от $2^{1/\varepsilon}$ множителя и за всеки от тях е изпълнено

$$\frac{l_i + 1}{p_i^{\varepsilon l_i}} \leq \frac{l_i + 1}{2^{\varepsilon l_i}} \leq \frac{2 l_i}{\frac{1}{2} \varepsilon l_i} = \frac{4}{\varepsilon}$$

(тук използувахме, че за всяко $x \in \mathbb{R}$, $x > 0$ е изпълнено $2^x = e^{x \ln 2} > 1 + x \ln 2 > \frac{x}{2}$). Следователно имаме

$$U \leq \Big(\frac{4}{\varepsilon} \Big)^{2^{1/\varepsilon}} .$$

Решението на задачата следва от горните оценки за U и V.

Задача 138. Да се докаже, че за всяка константа $A > 0$ съществува строго растяща редица от естествени числа $n_1, n_2, \ldots$, такава че

$$\lim_{m\to\infty} \frac{\tau(n_m)}{(\ln n_m)^A} = \infty\,.$$

Решение: Нека $l = [A] + 2$ и да означим с H_l произведението на първите l прости числа. Полагаме $n_m = {H_l}^m$, $m = 1, 2, \ldots$. От задача 134 следва, че $\tau(n_m) = (m+1)^l$. Тогава

$$\frac{\tau(n_m)}{(\ln n_m)^A} = \frac{(m+1)^l}{(m\,\ln H_l)^A} \geq m^{l-A}\,(\ln H_l)^{-A} \geq m\,(\ln H_l)^{-A}\,,$$

откъдето твърдението следва непосредствено.

Забележка: Твърденията, както в задача 137, така и в задача 138 могат да бъдат усилени. По–точно, може да се докаже, че за всяко $\varepsilon \in \mathbb{R}$, $\varepsilon > 0$ е изпълнено

$$\tau(n) < 2^{(1+\varepsilon)\frac{\ln n}{\ln\ln n}}$$

при достатъчно големи n. От друга страна, за безбройно много стойности на n е в сила

$$\tau(n) > 2^{(1-\varepsilon)\frac{\ln n}{\ln\ln n}}\,.$$

Задача 139. Нека $k, m \in \mathbb{N}$, $k \geq 2$ и да означим чрез $t(k,m)$ броя на решенията на уравнението

$$x_1y_1 + x_2y_2 + \cdots + x_ky_k = m$$

в числа $x_1, y_1, \ldots, x_k, y_k \in \mathbb{N}$. Да се докаже, че при всяко $\varepsilon \in \mathbb{R}$, $\varepsilon > 0$ и при фиксирано k е изпълнено

$$\lim_{m\to\infty} \frac{t(k,m)}{m^{k-1+\varepsilon}} = 0\,.$$

Вярно ли е горното равенство при $\varepsilon = 0$?

Решение: Като използуваме определение 29 и задача 137, получаваме, че за всяко $\delta > 0$ е изпълнено

$$t(k,m) = \sum_{\substack{n_1,\ldots,n_k \in \mathbb{N} \\ n_1+\cdots+n_k=m}} \tau(n_1)\,\ldots\,\tau(n_k) \;\leq\; C(\delta)^k \sum_{\substack{n_1,\ldots,n_k \in \mathbb{K} \\ n_1+\cdots+n_k=m}} n_1^{\delta}\ldots n_k^{\delta} \;\leq$$

$$\leq C(\delta)^k\, m^{k\delta} \sum_{\substack{n_1,\ldots,n_k \in \mathbb{N} \\ n_1+\cdots+n_k=m}} 1 \;\leq\; C(\delta)^k\, m^{k\delta} \sum_{n_1,\ldots,n_{k-1} \leq m} 1 \;\leq$$

$$\leq (k-1)\, C(\delta)^k\, m^{k-1+k\delta}\,.$$

Полагаме $\delta = \varepsilon(2k)^{-1}$ и получаваме

$$\frac{t(k,m)}{m^{k-1+\varepsilon}} \leq \frac{(k-1)\, C(\delta)^k}{m^{\varepsilon/2}}\,,$$

откъдето твърдението следва непосредствено.

Ако $\varepsilon = 0$ даденото равенство не е възможно, понеже при достатъчно голямо m имаме

$$t(k,m) \geq \sum_{\substack{n_1,\ldots,n_k \in \mathbb{N} \\ n_1+\cdots+n_k=m}} 1 \geq \sum_{n_1,\ldots,n_{k-1} \leq \frac{m}{k}} 1 \geq \left(\frac{m}{2k}\right)^{k-1}.$$

Определение 30. Нека $k, n \in \mathbb{N}$. Чрез $\tau_k(n)$ означаваме броя на наредените k-торки $m_1, m_2, \ldots m_k \in \mathbb{N}$, такива че $m_1 m_2 \ldots m_k = n$.

Задача 140. Да се докаже, че $\tau_1(n) = 1$, $\tau_2(n) = \tau(n)$ и, че при $k \in \mathbb{N}$, $k \geq 2$ е изпълнено $\tau_k(n) = \sum_{d|n} \tau_{k-1}(d)$.

Упътване: Първите две твърдения са очевидни, а третото следва непосредствено от определение 30.

Задача 141. Да се докаже, че при всяко фиксирано $k \in \mathbb{N}$ числовата функция $\tau_k(n)$ е мултипликативна по отношение на n.

Упътване: Да се използуват задачи 104 и 140.

Задача 142. Да се изчисли $\tau_k(n)$, ако е известно каноничното разлагане на числото n.

Упътване: Първо да се разгледа случая $n = p^l$, където p е просто и $l \in \mathbb{N}$, след което да се използува задача 141.

Отговор: Ако каноничното разлагане е $n = p_1^{l_1} p_2^{l_2} \dots p_s^{l_s}$, то

$$\tau_k(n) = \prod_{i=1}^{s} \frac{(l_i+1)(l_i+2)\dots(l_i+k-1)}{(k-1)!}\,.$$

Задача 143. Да се докаже, че за всяко $k \in \mathbb{N}$, $k \geq 2$ и за всяко $\varepsilon \in \mathbb{R}$, $\varepsilon > 0$ съществува константа $C(k,\varepsilon) > 0$, такава че при $n \in \mathbb{N}$ е в сила неравенството

$$\tau_k(n) \leq C(k,\varepsilon)\, n^{\varepsilon}\,.$$

Решение: Твърдението следва от тривиалното неравенство $\tau_k(n) \leq \tau(n)^{k-1}$ и от задача 137.

Определение 31. Нека $n \in \mathbb{N}$ и $\alpha \in \mathbb{C}$. Определяме $\sigma_\alpha(n) = \sum_{d|n} d^\alpha$. и, в частност, означаваме $\sigma(n) = \sigma_1(n)$.

Задача 144. Да се докаже, че за всяко $\alpha \in \mathbb{C}$ функцията $\sigma_\alpha(n)$ е мултипликативна по отношение на n.

Задача 145. Да се изчисли $\sigma_\alpha(n)$ при $\alpha \in \mathbb{C}$, $\alpha \neq 0$, ако е известно каноничното разлагане на числото n.

Отговор: Ако каноничното разлагане е $n = p_1^{l_1} \dots p_s^{l_s}$, то

$$\sigma_\alpha(n) = \prod_{i=1}^{s} \frac{p_i^{\alpha(l_i+1)} - 1}{p_i^{\alpha} - 1}\,.$$

Задача 146. Да се докаже, че съществува константа $A > 0$, такава че за всяко $n \in \mathbb{N}$ е изпълнено

$$A \leq \frac{\sigma(n)\,\varphi(n)}{n^2} \leq 1\,.$$

Решение: Можем да считаме, че $n > 1$ и че каноничното му разлагане е $n = p_1^{l_1} \dots p_s^{l_s}$, като $l_i \in \mathbb{N}$. Да положим $f(n) = \sigma(n)\,\varphi(n)\,n^{-2}$. Като използуваме задачи 130 и 145, получаваме $f(n) = \prod_{i=1}^{s} \left(1 - p_i^{-l_i-1}\right)$. Тогава имаме

$$1 \geq f(n) \geq \prod_{i=1}^{s} \left(1 - \frac{1}{p_i^2}\right) \geq \prod_{i=2}^{\infty} \left(1 - \frac{1}{i^2}\right)\,.$$

Тъй като последното произведение е сходящо, твърдението е доказано.

7 Дзета–функция на Риман

Определение 32. За всяко $s \in \mathbb{C}$, за което $Re\, s > 1$, определяме *дзета–функцията на Риман* чрез формулата

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}\,.$$

Забележка: Дзета–функцията на Риман е една от най–важните функции в теорията на числата. Риман е доказал, че $\zeta(s)$ се продължава аналитично до мероморфна функция в $\mathbb{C}$, която притежава единствен полюс в точката $s = 1$. Риман е установил, че $\zeta(s)$ се анулира в точките $s = -2, -4, -6, \ldots$ (наречени *тривиални нули*). Освен тях, $\zeta(s)$ притежава безбройно много *нетривиални нули* в ивицата $0 \leq Re\, s \leq 1$. Известната хипотеза на Риман гласи, че всички те лежат върху правата $Re\, s = \frac{1}{2}$. Тази хипотеза не е доказана или опровергана до ден днешен. Счита се, че това е един от най–трудните и най–важните проблеми в математиката.

Някои елементарни свойства на $\zeta(s)$, които илюстрират връзката ѝ с числовите функции, са дадени в следващите задачи.

Задача 147. Нека $\delta \in \mathbb{R}$, $\delta > 1$. Да се провери, че редът, който представя $\zeta(s)$, е абсолютно и равномерно сходящ в полуравнината $Re\, s \geq \delta$ и че дзета–функцията е аналитична в полуравнината $Re\, s > 1$.

Решение: Първото твърдение е очевидно, а второто е следствие от теоремата на Вайершрас за равномерно сходящи редове от аналитични функции.

Задача 148. Да се докаже, че при $Re\, s > 1$ е в сила тъждеството

$$\zeta(s) = \prod_{p} \left(1 - \frac{1}{p^s}\right)^{-1}\,.$$

Упътване: Да се използуват задача 108 и определение 32.

Задача 149. Да се докаже, че $\zeta(s) \neq 0$ при $Re\, s > 1$.

Решение: Ако $Re\, s = \sigma > 1$, то от задача 108 следва, че

$$\Big|\prod_p \Big(1 - \frac{1}{p^s}\Big)\Big| \leq \prod_p \Big(1 + \frac{1}{p^\sigma}\Big) \leq \sum_{n=1}^{\infty} \frac{1}{n^\sigma} = \zeta(\sigma)\,.$$

Остава да приложим задача 148 и твърдението е доказано.

Забележка: Може да се докаже, че $\zeta(2) = \frac{\pi^2}{6}$, $\zeta(4) = \frac{\pi^4}{90}$ и се знае, че за всяко $k \in \mathbb{N}$ имаме $\zeta(2k) = c_k \pi^{2k}$, където $c_k \in \mathbb{Q}$. Оттук, като следствие от теоремата на Линдеман за трансцендентност на числото π, се получава, че за всяко $k \in \mathbb{N}$ числото $\zeta(2k)$ е трансцендентно.

Много по–слабо са изучени числата от вида $\zeta(2k+1)$, където $k \in \mathbb{N}$. Известно е, че $\zeta(3)$ е ирационално (това е доказано от Апери), но подобен факт не е установен за никое друго от числата $\zeta(2k+1)$. Интересен резултат в това направление е получен неотдавна от Зудилин. През 2001 г. той доказа, че поне едно от числата $\zeta(5)$, $\zeta(7)$, $\zeta(9)$, $\zeta(11)$ е ирационално.

Задача 150. Да се докаже, че при $Re\, s > 1$ е в сила тъждеството

$$\frac{1}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}\,.$$

Решение: Като използуваме теоремата за умножаване на абсолютно сходящи редове и определение 25, получаваме

$$\zeta(s) \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \sum_{k=1}^{\infty} \sum_{n=1}^{\infty} \frac{\mu(n)}{(kn)^s} = \sum_{m=1}^{\infty} \frac{1}{m^s} \sum_{\substack{k,n \in \mathbb{N} \\ kn = m}} \mu(n)$$

$$= \sum_{m=1}^{\infty} \frac{1}{m^s} \sum_{n|m} \mu(n) = 1\,.$$

Задача 151. Да се докаже, че при $Re\, s > 1$ е изпълнено

$$\zeta'(s) = -\sum_{n=1}^{\infty} \frac{\ln n}{n^s}\,.$$

Решение: Тъждеството следва от теоремата на Вайершрас за почленно диференциране на редове от аналитични функции.

Задача 152. Да се докаже, че при $Re\, s > 1$ е в сила тъждеството

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}\,.$$

Упътване: Да се установи, че редът $\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}$ е абсолютно сходящ в полуравнината $Re\, s > 1$ и да се умножи с реда, представящ $\zeta(s)$. По–нататък, да се работи както при решението на задача 150, като се използват определение 27 и задача 151.

Задача 153. Да се докаже, че при $Re\, s > 1$ е в сила тъждеството

$$\frac{\zeta(2s)}{\zeta(s)} = \prod_{p} \left(1 + \frac{1}{p^s}\right)^{-1}\,.$$

Упътване: Да се използува задача 148.

Задача 154. Нека $k \in \mathbb{N}$, $k \geq 2$. Да се докаже, че при $Re\, s > 1$ е в сила тъждеството

$$\zeta^k(s) = \sum_{n=1}^{\infty} \frac{\tau_k(n)}{n^s}\,.$$

Упътване: Да се използуват теоремата за умножаване на абсолютно сходящи редове и определение 30.

Задача 155. Да се докаже, че при $Re\, s > 2$ е в сила тъждеството

$$\frac{\zeta(s-1)}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\varphi(n)}{n^s}\,.$$

Задача 156. Да се докаже, че при $Re\, s > 2$ е в сила тъждеството

$$\zeta(s-1)\zeta(s) = \sum_{n=1}^{\infty} \frac{\sigma(n)}{n^s}\,.$$

Забележка: Редовете от определение 32 и задачи 150 – 156 са примери за така наречените *редове на Дирихле* . Те се определят чрез формулата

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s}\,,$$

където a_n, $n = 1, 2, 3, \ldots$ са произволни комплексни числа. Редовете на Дирихле имат важни приложения в теорията на числата. С тяхна помощ Дирихле е доказал, че ако $a, b \in \mathbb{N}$ и $(a, b) = 1$, то аритметичната прогресия $a + nb$, $n = 1, 2, 3, \ldots$ съдържа безбройно много прости числа.

8 Сравнения – основни свойства

Определение 33. Нека $m \in \mathbb{N}$ и $a, b \in \mathbb{Z}$. Казваме, че a *е сравнимо с* b *по модул* m и пишем $a \equiv b \pmod{m}$, ако $m \mid (a - b)$. Ако не е вярно, че a е сравнимо с b по модул m, ще казваме, че числата a и b са *несравними по модул* m и ще пишем $a \not\equiv b \pmod{m}$.

Примери: $33 \equiv 18 \pmod{5}$, $-29 \equiv 11 \pmod{8}$, $53 \not\equiv 3 \pmod{7}$, $46 \not\equiv -7 \pmod{17}$.

Задача 157. Нека $a, b, c \in \mathbb{Z}$ и $m \in \mathbb{N}$. Да се докажат свойствата:

а) $a \equiv a \pmod{m}$.

б) $a \equiv b \pmod{m} \implies b \equiv a \pmod{m}$.

в) $a \equiv b \pmod{m}, b \equiv c \pmod{m} \implies a \equiv c \pmod{m}$.

Задача 158. Нека $a, b, c, d \in \mathbb{Z}$, $m, n \in \mathbb{N}$. Да се докажат свойствата:

а) $a \equiv b \pmod{m} \implies a \pm c \equiv b \pm c \pmod{m}$,

б) $a \equiv b \pmod{m} \implies ac \equiv bc \pmod{m}$,

в) $a \equiv b \pmod{m}$, $c \equiv d \pmod{m} \implies a \pm c \equiv b \pm d \pmod{m}$,

г) $a \equiv b \pmod{m}$, $c \equiv d \pmod{m} \implies ac \equiv bd \pmod{m}$,

д) $a \equiv b \pmod{m} \implies a^n \equiv b^n \pmod{m}$.

Решение: Свойства а) и б) се получават непосредствено от определение 33. Свойство в) следва от равенството $(a \pm c) - (b \pm d) = (a - b) \pm (c - d)$. Доказателството на г) следва от тъждеството $ac - bd = (a - b)c + b(c - d)$. Свойство д) следва от г).

Задача 159. Нека $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$ и нека $d \in \mathbb{N}$ е общ делител на a, b и m. Да се докаже, че $a \equiv b \pmod{m}$ тогава и само тогава, когато е изпълнено $\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{m}{d}}$.

Решение: Твърдението следва от определение 33 и от равенството

$$\frac{\frac{b}{d} - \frac{a}{d}}{\frac{m}{d}} = \frac{b-a}{m}.$$

Задача 160. Нека $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$ и $a \equiv b \pmod{m}$. Да се докаже, че ако $d \in \mathbb{N}$ е общ делител на a и b такъв, че $(d, m) = 1$, то

$$\frac{a}{d} \equiv \frac{b}{d} \pmod{m}.$$

Решение: Тъй като $m \mid d\left(\frac{b}{d} - \frac{a}{d}\right)$ и $(d, m) = 1$, то от задача 9 следва, че $m \mid \left(\frac{b}{d} - \frac{a}{d}\right)$.

Задача 161. Нека $a, b \in \mathbb{Z}$ и нека числата $n_1, \ldots, n_s \in \mathbb{N}$ са две по две взаимно прости. Да се докаже, че сравнението

$$a \equiv b \pmod{n_1 \ldots n_s}$$

е еквивалентно на системата от сравнения

$$a \equiv b \pmod{n_1}, \quad \ldots \quad , \quad a \equiv b \pmod{n_s}.$$

Решение: Твърдението следва от задача 16 и от определение 33.

Определение 34. Нека $m \in \mathbb{N}$ и $\mathcal{M} \subset \mathbb{Z}$. Казваме, че $\mathcal{M}$ е *пълна система от остатъци по модул* m (по–нататък ще пишем п.с.о. $\pmod{m}$), ако са налице условията:

а) $a, b \in \mathcal{M}$, $a \neq b \implies a \not\equiv b \pmod{m}$,

б) за всяко $x \in \mathbb{Z}$ съществува $c \in \mathcal{M}$, такова че $x \equiv c \pmod{m}$.

Задача 162. Да се докаже, че всяка п.с.о. $\pmod{m}$ се състои от m на брой числа.

Задача 163. Да се докаже, че всяка система от m на брой цели числа, които са две по две несравними по модул m, образува п.с.о. $\pmod{m}$.

Задача 164. Да се провери, че ако $m \in \mathbb{N}$, то

а) $1, 2, \ldots, m$ е п.с.о. $\pmod{m}$,

б) ако m е нечетно, то $0, \pm 1, \pm 2, \ldots, \pm\frac{m-1}{2}$ е п.с.о. $\pmod{m}$,

в) ако m е четно, то $-\frac{m}{2}+1, -\frac{m}{2}+2, \ldots, -1, 0, 1, \ldots \frac{m}{2}$ е п.с.о. $\pmod{m}$.

Задача 165. Нека $m \in \mathbb{N}$, $a, b \in \mathbb{Z}$, като $a \neq 0$ и $(a, m) = 1$. Да се докаже, че ако x пробягва п.с.о. $(\mathrm{mod}\ m)$, то $ax + b$ пробягва също п.с.о. $(\mathrm{mod}\ m)$.

Решение: Твърдението следва от задачи 158, 160 и 163.

Задача 166. Нека са дадени $n_1, n_2 \in \mathbb{N}$, такива че $(n_1, n_2) = 1$. Да се докаже, че ако числата x_1 и x_2 пробягват пълни системи от остатъци съответно по модули n_1 и n_2, то тогава числата $x_1 n_2 + x_2 n_1$ пробягват п.с.о. $(\mathrm{mod}\ n_1 n_2)$.

Упътване: Да се използува, че ако

$$x_1 n_2 + x_2 n_1 \equiv x_1' n_2 + x_2' n_1 \pmod{n_1 n_2},$$

то $x_1 n_2 \equiv x_1' n_2 \pmod{n_1}$, откъдето $x_1 \equiv x_1' \pmod{n_1}$ вследствие на задача 160. Но тъй като x_1, x_1' са от дадена п.с.о. $(\mathrm{mod}\ n_1)$, то $x_1 = x_1'$. Аналогично получаваме, че $x_2 = x_2'$. Остава да забележим, че броят на числата $x_1 n_2 + x_2 n_1$ е $n_1 n_2$ и да приложим задача 163.

Задача 167. Нека $n, m \in \mathbb{N}$. Да се докаже, че ако числата x и y пробягват пълни системи от остатъци съответно по модули n и m, то тогава числата $x + yn$ пробягват п.с.о. $(\mathrm{mod}\ nm)$.

Упътване: Да се използуват задачи 159, 163 и определение 34.

Задача 168. Нека $n, m \in \mathbb{N}$, $x_0 \in \mathbb{Z}$ и нека $\mathcal{M}$ е п.с.о. $(\mathrm{mod}\ nm)$. Да се докаже, че съществуват точно m на брой числа $y \in \mathbb{Z}$, за които $x_0 + yn \in \mathcal{M}$.

Определение 35. Нека $m \in \mathbb{N}$ и $\mathcal{R} \subset \mathbb{Z}$. Казваме, че $\mathcal{R}$ е *редуцирана система от остатъци по модул* m (ще записваме р.с.о. $(\mathrm{mod}\ m)$), ако са налице условията:

а) $a \in \mathcal{R} \implies (a, m) = 1$,

б) $a, b \in \mathcal{R}$, $a \neq b \implies a \not\equiv b \pmod{m}$,

в) за всяко $x \in \mathbb{Z}$, такова че $(x, m) = 1$ съществува $c \in \mathcal{R}$, за което $x \equiv c \pmod{m}$.

Пример: Числата $1, 3, 7, 9$ образуват р.с.о. $(\mathrm{mod}\ 10)$.

Задача 169. Нека $m \in \mathbb{N}$. Да се докаже, че всяка р.с.о. $(\mathrm{mod}\ m)$ се състои точно от $\varphi(m)$ на брой елемента.

Задача 170. Да се докаже, че от всяка п.с.о. $(\mathrm{mod}\ m)$ може да се избере една единствена р.с.о. $(\mathrm{mod}\ m)$. Обратно, всяка р.с.о. $(\mathrm{mod}\ m)$ може да бъде разширена до п.с.о. $(\mathrm{mod}\ m)$.

Задача 171. Нека $m \in \mathbb{N}$. Да се докаже, че всяка система от $\varphi(m)$ на брой цели числа, които са две по две несравними по модул m и са взаимно прости с m, образува р.с.о. $(\mathrm{mod}\ m)$.

Задача 172. Нека $m \in \mathbb{N}$, $a \in \mathbb{Z}$, като $a \neq 0$ и $(a, m) = 1$. Да се докаже, че ако x пробягва р.с.о. $(\mathrm{mod}\ m)$, то ax пробягва също р.с.о. $(\mathrm{mod}\ m)$.

Упътване: Да се използуват задачи 160 и 171.

Задача 173. Нека са дадени $n_1, n_2 \in \mathbb{N}$, такива че $(n_1, n_2) = 1$. Да се докаже, че ако числата x_1 и x_2 пробягват редуцирани системи от остатъци съответно по модули n_1 и n_2, то числата $x_1 n_2 + x_2 n_1$ пробягват р.с.о. $(\mathrm{mod}\ n_1 n_2)$.

Упътване: Да се разсъждава както при решението на задача 166, като се използува задача 171.

Забележка: От задачи 169 и 173 получаваме друго доказателство за мултипликативността на функцията на Ойлер.

9 Теореми на Ферма и Ойлер

Задача 174. Нека $m \in \mathbb{N}$, $a \in \mathbb{Z}$ и $(a, m) = 1$. Да се докаже, че е в сила сравнението

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Решение: Нека $a_1, a_2, \ldots, a_{\varphi(m)}$ е р.с.о. $(\mathrm{mod}\ m)$. Според задача 172 числата $aa_1, aa_2, \ldots, aa_{\varphi(m)}$ също образуват р.с.о. $(\mathrm{mod}\ m)$. Тогава имаме

$$a_1 a_2 \ldots a_{\varphi(m)} \equiv (aa_1)(aa_2)\ldots(aa_{\varphi(m)}) \equiv a^{\varphi(m)} a_1 a_2 \ldots a_{\varphi(m)} \pmod{m}.$$

Тъй като $(n, a_1 a_2 \ldots a_{\varphi(m)}) = 1$, то използувайки задача 160 получаваме доказателство на твърдението.

Забележка: Резултатът от задача 174 е известен като *теорема на Ойлер*.

Задача 175. Нека $a \in \mathbb{Z}$ и p е просто число. Да се докаже, че е в сила сравнението

$$a^p \equiv a \pmod{p}.$$

Решение: Ако $p \mid a$, то твърдението е очевидно. Ако пък $p \nmid a$ сравнението е еквивалентно на $a^{p-1} \equiv 1 \pmod{p}$, което е следствие от задача 174.

Забележка: Резултатът от задача 175 е известен като *малка теорема на Ферма*.

Задача 176. Нека $a_1, \ldots, a_s \in \mathbb{Z}$ и p е просто число. Да се докаже, че е в сила сравнението

$$(a_1 + \cdots + a_s)^p \equiv a_1^p + \cdots + a_s^p \pmod{p}.$$

Решение: Резултатът следва от задача 175.

Забележка: Както видяхме, малката теорема на Ферма представлява частен случай на теоремата на Ойлер. В следващата задача ще дадем директно доказателство на малката теорема на Ферма и след това с нейна помощ ще получим ново доказателство на теоремата на Ойлер.

Задача 177. Да се даде директно доказателство на малката теорема на Ферма.

Решение: Очевидно, достатъчно е да разгледаме случая $a \in \mathbb{N}$. Ако $a = 1$ твърдението е очевидно. Нека $a > 1$ и да допуснем, че твърдението е вярно за числото $a - 1$. Биномната формула на Нютон ни дава

$$a^p = \big((a-1)+1\big)^p = (a-1)^p + \sum_{k=1}^{p-1} \binom{p}{k} (a-1)^{p-k} + 1\,.$$

Като използуваме задача 45 и индукционното допускане, получаваме

$$a^p \equiv (a-1)^p + 1 \equiv (a-1) + 1 \equiv a \pmod{p}.$$

Задача 178. Нека p е просто число и $l \in \mathbb{N}$. Да се докаже, че ако за някое $m \in \mathbb{Z}$ е в сила $m \equiv 1 \pmod{p^l}$, то тогава $m^p \equiv 1 \pmod{p^{l+1}}$.

Упътване: По условие имаме $m = 1 + kp^l$ за някое $k \in \mathbb{Z}$. Да се развие $m^p = (1 + kp^l)^p$ по формулата на Нютон и да се използува задача 45.

Задача 179. Да се докаже теоремата на Ойлер като се използуват малката теорема на Ферма и задача 178.

Решение: Нека p е просто число, $a \in \mathbb{Z}$ и нека $p \nmid a$. Според задача 177 имаме $a^{p-1} \equiv 1 \pmod{p}$. Ако $l \in \mathbb{N}$, то прилагаме $l-1$ пъти резултата от задача 178 и получаваме последователно

$$a^{p(p-1)} \equiv 1 \pmod{p^2}, \quad \ldots, \quad a^{p^{l-1}(p-1)} \equiv 1 \pmod{p^l},$$

т.е. $a^{\varphi(p^l)} \equiv 1 \pmod{p^l}$. Нека $n \in \mathbb{N}$, $(a,n) = 1$ и $n > 1$ (случаят $n = 1$ е тривиален). Да предположим, че n има канонично разлагане $n = p_1^{l_1} \ldots p_s^{l_s}$, като $l_i \in \mathbb{N}$. Както видяхме, имаме $a^{\varphi(p_i^{l_i})} \equiv 1 \pmod{p_i^{l_i}}$. Да забележим, че $\varphi(p_i^{l_i}) \mid \varphi(n)$. Тогава от задача 158 д) получаваме $a^{\varphi(n)} \equiv 1 \pmod{p_i^{l_i}}$ и тъй като това сравнение е налице при $1 \leq i \leq s$, то твърдението следва от задача 161.

Задача 180. Да се докаже, че ако $a, n \in \mathbb{N}$, $n \geq 3$ и $2 \nmid a$, то

$$a^{2^{n-2}} \equiv 1 \pmod{2^n}.$$

Решение: При $n = 3$ твърдението се проверява непосредствено. Ако $n > 3$, то неколкократно прилагаме задача 178.

Задача 181. Нека $a, m \in \mathbb{N}$ и $a^{m-1} \equiv 1 \pmod{m}$. Вярно ли е, че числото m е просто?

Решение: В общия случай не е вярно. Да разгледаме, например, числото $m = 561 = 3 \cdot 11 \cdot 17$ и нека $a \in \mathbb{N}$ е такова, че $561 \nmid a$. Имаме

$$a^2 \equiv 1 \pmod{3}, \quad a^{10} \equiv 1 \pmod{11}, \quad a^{16} \equiv 1 \pmod{17}.$$

Тъй като $2 \mid 560$, $10 \mid 560$, $16 \mid 560$, то

$$a^{560} \equiv 1 \pmod{3}, \quad a^{560} \equiv 1 \pmod{11}, \quad a^{560} \equiv 1 \pmod{17}.$$

Тогава от задача 161 получаваме $a^{560} \equiv 1 \pmod{561}$.

Забележка: Казваме, че съставното числото $m \in \mathbb{N}$ е *псевдо–просто* по отношение на $a \in \mathbb{N}$, ако е в сила $a^{m-1} \equiv 1 \pmod{m}$. Съставно число $m \in \mathbb{N}$, което е псевдо–просто по отношение на всяко $a \in \mathbb{N}$, такова че $(a, m) = 1$, се нарича *число на Кармикаел*. Например, числотто 561 е число на Кармикаел.

Може да се докаже сравнително лесно, че за всяко $a \in \mathbb{N}$, $a > 1$ съществуват безбройно много числа, които са псевдо–прости по отношение на a. Доказателството за съществуване на безбройно много числа на Кармикаел е много по–сложно и бе намерено едва през 1994 г. от Алфорд, Гренвил и Померанс.

10 Сравнения и системи сравнения с едно неизвестно

Определение 36. Нека $n \in \mathbb{N}$ и $f \in \mathbb{Z}[x]$. Всяко число $x \in \mathbb{Z}$, което удовлетворява сравнението $f(x) \equiv 0 \pmod{n}$, се нарича негово решение. Да се реши това сравнение означава да се намерят всички негови решения.

Забележка: Както обикновено, $\mathbb{Z}[x]$ означава съвкупността от полиномите на x с цели коефициенти.

Определение 37. Нека $n, m \in \mathbb{N}$ и $f, g \in \mathbb{Z}[x]$. Казваме, че сравненията $f(x) \equiv 0 \pmod{n}$ и $g(x) \equiv 0 \pmod{m}$ са *еквивалентни*, ако множествата от решенията им съвпадат.

Задача 182. Нека $n \in \mathbb{N}$ и $f \in \mathbb{Z}[x]$. Да се докажат свойствата

а) Ако $x_1 \in \mathbb{Z}$ е решение на сравнението

$$f(x) \equiv 0 \pmod{n} \qquad (i)$$

и ако $x_2 \equiv x_1 \pmod{n}$, то x_2 също е решение на сравнението (i).

б) Ако $\mathcal{M}$ е п.с.о. $\pmod{n}$, то всички решения на сравнението (i) се получават като към решенията, принадлежащи на $\mathcal{M}$ се присъединят всички цели числа, сравними с някое от тях по модул n.

в) Ако $\mathcal{M}$ и $\mathcal{M}'$ са п.с.о. $(\mathrm{mod}\ n)$, то броят на числата от $\mathcal{M}$, които удовлетворяват сравнението (i), е равен на броя на числата от $\mathcal{M}'$, които удовлетворяват същото сравнение.

Забележка: От задача 182 се вижда, че за да решим сравнението (i) е достатъчно да намерим решенията му, които се намират в някоя п.с.о. $(\mathrm{mod}\ n)$. За конкретни $n \in \mathbb{N}$ и $f \in \mathbb{Z}[x]$ решаването на (i) се свежда до извършването на краен брой проверки.

Ако числото n или степента и модулите на коефициентите на f са твърде големи, то от съществено значение е изчисленията да се извършват по оптимален алгоритъм — в противен случай дори и използуването на компютър не гарантира решаването на задачата в обозримо време.

Задача 183. Да се решат сравненията

а) $x^8 - 1 \equiv 0 \pmod{15}$,

б) $x^2 + 1 \equiv 0 \pmod{11}$.

Отговор: а) $x \equiv 1, 2, 4, 7, 8, 11, 13, 14 \pmod{15}$; б) няма решение.

Определение 38. Нека $n \in \mathbb{N}$ и $f \in \mathbb{Z}[x]$. Означаваме чрез $r_f(n)$ броя на решенията на $f(x) \equiv 0 \pmod{n}$, намиращи се в някоя п.с.о. $(\mathrm{mod}\ n)$. Величината $r_f(n)$ се нарича брой на решенията на сравнението.

Забележка: Коректността на определение 38 е следствие от задача 182.

Задача 184. Да се определи броя на решенията на сравненията от задача 183.

Отговор: а) 8; б) 0.

Задача 185. Да се докаже, че за всеки полином $f \in \mathbb{Z}[x]$ функцията $r_f(n)$ е мултипликативна по отношение на n.

Решение: Очевидно $r_f(1) = 1$. Нека $n_1, n_2 \in \mathbb{N}$ и $(n_1, n_2) = 1$. Ако $\mathcal{M}_1$ и $\mathcal{M}_2$ са п.с.о. съответно по модули n_1 и n_2, то като използуваме задачите 161, 165, 166 и определение 38, получаваме

$$r_f(n_1 n_2) = \sum_{\substack{x_1 \in \mathcal{M}_1 \\ f(x_1 n_2 + x_2 n_1) \equiv 0 \pmod{n_1 n_2}}} \sum_{x_2 \in \mathcal{M}_2} 1 = \sum_{\substack{x_1 \in \mathcal{M}_1 \\ f(x_1 n_2) \equiv 0 \pmod{n_1} \\ f(x_2 n_1) \equiv 0 \pmod{n_2}}} \sum_{x_2 \in \mathcal{M}_2} 1 = r_f(n_1)\, r_f(n_2)\,.$$

11 Линейни сравнения

Задача 186. Нека $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$ и нека $d = (a, n)$. Да се докажат свойствата:

а) Ако $d \nmid b$, то сравнението $ax \equiv b \pmod{n}$ няма решение.

б) Ако $d \mid b$, то сравнението $ax \equiv b \pmod{n}$ има d на брой решения.

Решение: Твърдението а) е очевидно. За да докажем б) полагаме $a = a_1 d$, $b = b_1 d$ и $n = n_1 d$. Имаме $(a_1, n_1) = 1$. Като използуваме задача 159, виждаме, че даденото сравнение е еквивалентно на сравнението $a_1 x \equiv b_1 \pmod{n_1}$. Според задача 165, ако x пробягва числата $1, 2, \ldots, n_1$, то числата $a_1 x$ образуват п.с.о. $\pmod{n_1}$, следователно измежду $1, 2, \ldots, n_1$ има единствено число x_1, за което $a_1 x_1 \equiv b_1 \pmod{n_1}$. Тогава измежду числата $1, 2, \ldots, n$ точно d на брой, а именно

$$x_1\,,\ x_1 + n_1\ x_1 + 2n_1\,, \ldots\,,\ x_1 + (d-1)n_1\,,$$

са решения на $ax \equiv b \pmod{n}$.

Задача 187. Нека $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$ и нека $(a, n) = 1$. Да се докаже, че решението на сравнението $ax \equiv b \pmod{n}$ се дава чрез формулата $x \equiv a^{\varphi(n)-1} b \pmod{n}$.

Решение: Твърдението следва непосредствено от задача 174.

Забележка: От решенията на задачи 186 и 187 виждаме, че решенията на сравнение от първа степен с едно неизвестно се дават в явен вид. За практиката е важно да можем да намираме решенията, които се намират в „обичайни“ п.с.о. $\pmod{n}$, например системите от задача 164.

Задача 188. Като се използува задача 187 да се намерят решенията на сравнението $109x \equiv 23 \pmod{312}$, принадлежащи на п.с.о. $\pmod{312}$, състояща се от числата $1, 2, \ldots, 312$.

Решение: Имаме $(109, 312) = 1$, следователно сравнението има едно решение. Тъй като $312 = 2^3 \cdot 3 \cdot 13$, то $\varphi(312) = \varphi(8) \cdot \varphi(3) \cdot \varphi(13) = 4 \cdot 2 \cdot 12 = 96$. От задача 187 намираме, че решенията се задават чрез $x \equiv 109^{95} \cdot 23 \pmod{312}$. Лесно се вижда, че $109^2 \equiv 25 \pmod{312}$. Тогава

$109^{95} \equiv 109 \cdot 25^{47} \pmod{312}$. По–нататък $25^2 = 625 \equiv 1 \pmod{312}$, следователно $25^{47} \equiv 25 \pmod{312}$. От горните изчисления окончателно намираме $x \equiv 109 \cdot 25 \cdot 23 \equiv 275 \pmod{312}$.

Забележка: Изложеният метод за решаване на линейни сравнения за практически цели не е много удобен, най–малкото понеже е неоходимо да намерим каноничното разлагане на модула на сравнението, а при големи числа за това са необходими много изчисления.

Задача 189. а) Да се намери бърз алгоритъм за намиране решенията на $ax \equiv b \pmod{n}$, които се намират в „обичайни“ п.с.о. $\pmod{n}$

б) С помощта на този алгоритъм да се реши задача 188.

Упътване: Да отбележим, че още при изчисляването на (a, n), ние прилагаме алгоритъма на Евклид, който е бърз и удобен за реализация.

Да разгледаме, например, случая $(a, n) = 1$ (общият случай се разглежда аналогично). Можем да считаме също, че $1 < a < n$. Полагаме $r_{-1} = n$, $r_0 = a$. Като приложим алгоритъма на Евклид, намираме $q_\nu, r_\nu \in \mathbb{Z}$, $1 \leq \nu \leq s+2$, такива че

$$r_\nu = q_{\nu+2} r_{\nu+1} + r_{\nu+2} \qquad \text{при} \qquad -1 \leq \nu \leq s \tag{i}$$

и $1 = r_{s+2} < r_{s+1} < \cdots < r_1 < r_0 = a$. Полагаме $P_0 = 1$, $P_1 = -q_1$. Очевидно имаме

$$P_\nu a \equiv r_\nu \pmod{n} \tag{ii}$$

при $\nu = 0, 1$. Нека $j \leq s+1$. Да допуснем, че сме определили $P_\nu \in \mathbb{Z}$, така че при $0 \leq \nu \leq j$ да е в сила (ii). Разглеждаме последните две сравнения:

$$P_{j-1} a \equiv r_{j-1} \pmod{n}, \qquad P_j a \equiv r_j \pmod{n}.$$

Към първото от тях прибаваме второто, умножено с $-q_{j+1}$. Използувайки (i) получаваме $P_{j+1} a \equiv r_{j+1} \pmod{n}$, където $P_{j+1} = P_{j-1} - q_{j+1} P_j$, с което конструкцията на редицата от числа P_ν е завършена. Имаме $P_{s+2} a \equiv r_{s+1} \equiv 1 \pmod{n}$, следователно решението на даденото сравнение се задава чрез $x \equiv P_{s+2} b \pmod{n}$.

б) За да решим сравнението $109x \equiv 23 \pmod{312}$, прилагаме алгоритъма на Евклид и намираме $312 = 2 \cdot 109 + 94$, $109 = 1 \cdot 94 + 15$, $94 = 6 \cdot 15 + 4$, $15 = 3 \cdot 4 + 3$, $4 = 1 \cdot 3 + 1$.

Оттук следва, че $(312, 109) = 1$. Използувайки метода, предложен в а), получаваме последователно сравненията $(-2) \cdot 109 \equiv 94 \pmod{312}$, $3 \cdot 109 \equiv 15 \pmod{312}$, $(-20) \cdot 109 \equiv 4 \pmod{312}$, $63 \cdot 109 \equiv 3 \pmod{312}$, $(-83) \cdot 109 \equiv 1 \pmod{312}$. Решението на даденото сравнение се дава чрез $x \equiv -83 \cdot 23 \equiv -1909 \equiv 275 \pmod{312}$.

Забележка: Линейно сравнение се решава още по–бързо, ако делението с частно и остатък в алгоритъма на Евклид се извършва според правилото от задача 6.

Задача 190. Да се изработи алгоритъм за решаване на линейни сравнения, като се използува идеята от последната забележка.

Задача 191. Да се решат сравненията

а) $90x \equiv 168 \pmod{312}$,

б) $42x \equiv 32 \pmod{98}$,

в) $27x \equiv 19 \pmod{94}$.

Отговор: а) $x \equiv 40, 92, 144, 196, 248, 300 \pmod{312}$; б) няма решение; в) $x \equiv 39 \pmod{94}$.

Задача 192. Да се решат сравненията

а) $(x-5)(x-7) \equiv x^2 + x + 1 \pmod{111}$,

б) $(x+1)(x-2) \equiv (x+3)(x+2) + x + 7 \pmod{16}$,

в) $2(x+3) + 5 \equiv 5x + 1 \pmod{80}$.

12 Системи линейни сравнения

Задача 193. Нека $n_1, \ldots, n_k \in \mathbb{N}$ и $c_1, \ldots, c_k \in \mathbb{Z}$. Да се докаже, че необходимо и достатъчно условие за разрешимост на системата сравнения

$$x \equiv c_1 \pmod{n_1}, \ \ldots\ldots, \ x \equiv c_k \pmod{n_k} \qquad (i)$$

е наличието на условията

$$c_i \equiv c_j \pmod{(n_i, n_j)} \quad \text{за всички} \quad 1 \leq i < j \leq k\,. \qquad (ii)$$

В случай на разрешимост системата е еквивалентна на сравнение от вида

$$x \equiv c \pmod{[n_1, \ldots, n_k]}, \qquad (iii)$$

където $c \in \mathbb{Z}$ е число, което зависи от $n_1, \ldots, n_k, c_1, \ldots, c_k$.

Решение: Случаят $k = 1$ е тривиален, така че считаме, че $k > 1$.

Очевидно, ако системата (i) има решение, то условията (ii) са налице.

Нека сега са изпълнени условията (ii). По индукция ще определим числа $c^{(l)} \in \mathbb{Z}$, $1 \leq l \leq k$, такива, че

$$c^{(l)} \equiv c_i \pmod{n_i} \quad \text{при} \quad 1 \leq i \leq l\,. \qquad (iv)$$

Определяме $c^{(1)} = c_1$. Нека при $l \in \mathbb{N}$, $l < k$ сме определили числото $c^{(l)} \in \mathbb{Z}$, така че да е налице (iv). Полагаме

$$c^{(l+1)} = c^{(l)} + z[n_1, \ldots, n_l]\,, \qquad (v)$$

където $z \in \mathbb{Z}$ ще определим по–долу. Ясно е, че

$$c^{(l+1)} \equiv c^{(l)} \equiv c_i \pmod{n_i} \quad \text{при} \quad 1 \leq i \leq l\,. \qquad (vi)$$

Определяме z по такъв начин, че да е в сила и условието

$$c^{(l+1)} \equiv c_{l+1} \pmod{n_{l+1}}, \qquad (vii)$$

или все едно

$$z[n_1, \ldots, n_l] \equiv c_{l+1} - c^{(l)} \pmod{n_{l+1}}. \qquad (viii)$$

От задача 186 следва, че за разрешимостта на $(viii)$ относно z е достатъчно да имаме

$$c_{l+1} - c^{(l)} \equiv 0 \pmod{([n_1, \ldots, n_l], n_{l+1})}. \qquad (ix)$$

В сила е тъждеството

$$([n_1, \ldots, n_l], n_{l+1}) = [(n_1, n_{l+1}), \ldots, (n_l, n_{l+1})] \qquad (x)$$

(то е очевидно обобщение на равенството от задача 30 а)). От условията (ii) и от предположението, че $c^{(l)}$ удовлетворява (iv) получаваме

$$c_{l+1} - c^{(l)} \equiv c_{l+1} - c_i \equiv 0 \pmod{(n_{l+1}, n_i)} \quad \text{при } 1 \leq i \leq l\,. \qquad (xi)$$

Сравнението (ix) е следствие от (x), (xi) и от задача 25. Като определим $c^{(l+1)}$ чрез (v), където z удовлетворява $(viii)$, получаваме, че са налице условията (vi) и (vii). С това конструкцията на редицата $c^{(l)}$, $1 \leq l \leq k$, която удовлетворява (iv), е завършена.

Числото $c = c^{(k)}$ е решение на (i), с което разрешимостта на тази система е установена. Очевидно, всяко $x \in \mathbb{Z}$, което удовлетворя (iii), е решение на (i). От друга страна, ако $x \in \mathbb{Z}$ е някакво решение на (i), то $n_i \mid (x - c)$ при $1 \leq i \leq k$, следователно x удовлетворява (iii).

Забележка 1: Като следствие получаваме, че ако числата $n_1, \ldots, n_k$ са две по две взаимно прости, то системата (i) е разрешима и има единствено решение по модул $n_1 \ldots n_k$. Това твърдение е известно като *китайска теорема за остатъците*.

Забележка 2: Решението на задача 193 ни дава метод за решаване на система от вида (i).

Забележка 3: Съществува критерий за разрешимост и на по–общи системи от вида $a_i x \equiv b_i \pmod{n_i}$, $1 \leq i \leq k$. При практическото им решаване е удобно да се решат всички сравнения, ако това е възможно, т.е. системата да се сведе до система от вида (i) (евентуално с други модули), която на свой ред се решава по описания по–горе начин.

Задача 194. Да се реши системата сравнения

$$6x \equiv 2 \pmod{10}, \quad 12x \equiv 6 \pmod{18}, \quad 16x \equiv 20 \pmod{28}. \qquad (i)$$

Решение: Като използуваме задача 159, виждаме, че системата (i) е еквивалентна на

$$3x \equiv 1 \pmod{5}, \qquad 2x \equiv 1 \pmod{3}, \qquad 4x \equiv 5 \pmod{7},$$

която на свой ред е еквивалентна на

$$x \equiv 2 \pmod{5}, \qquad x \equiv 2 \pmod{3}, \qquad x \equiv 3 \pmod{7}. \qquad (ii)$$

От първото сравнение на (ii) получаваме $x = 2 + 5y$ за някое $y \in \mathbb{Z}$. Заместваме във второто сравнение и получаваме $2 + 5y \equiv 2 \pmod{3}$, откъдето $y \equiv 0 \pmod{3}$, т.е. $y = 3z$ за някое $z \in \mathbb{Z}$. Тогава имаме $x = 2 + 15z$ и като заместим в третото сравнение на (ii), получаваме $2 + 15z \equiv 3 \pmod{7}$, откъдето $z \equiv 1 \pmod{7}$. Тогава $z = 1 + 7t$ за някое $t \in \mathbb{Z}$, следователно $x = 17 + 105t$. Получаваме, че решенията на системата (i) са числата $x \equiv 17 \pmod{105}$.

Задача 195. Да се решат системите сравнения

а) $36x \equiv 68 \pmod{308}$, $66x \equiv 84 \pmod{390}$;

б) $42x \equiv 66 \pmod{90}$, $44x \equiv 20 \pmod{84}$;

в) $5x \equiv 1 \pmod{6}$, $7x \equiv 9 \pmod{10}$, $11x \equiv 7 \pmod{15}$;

г) $x \equiv 13 \pmod{15}$, $x \equiv 4 \pmod{21}$, $x \equiv 18 \pmod{35}$.

Задача 196. Да се намери най–малкото естествено число, което при деление на 2, 3, 4, 5, 6 дава остатък единица и което се дели без остатък на 7.

Отговор: 301.

Задача 197. Да се намерят стойностите на параметъра $a \in \mathbb{Z}$, за които системата

$$x \equiv a \pmod{12}, \qquad x \equiv 2a \pmod{15}, \qquad x \equiv 3a \pmod{20}$$

има решение.

Задача 198. Да се докаже, че за всяко $k \in \mathbb{N}$ съществуват $x_0, y_0 \in \mathbb{N}$, такива че $(x_0 + h, y_0 + l) > 1$ за всички $h, l \in \mathbb{N}$, за които $h, l \leq k$.

Решение: Вземаме k^2 на брой различни прости числа и ги нареждаме в квадратна таблица. Да означим с m_i и M_j, $1 \leq i, j \leq k$, произведението от простите числа от i–тия ред, съответно j–тия стълб.

Нека $x_0 \in \mathbb{N}$ е решение на системата

$$x \equiv -i \pmod{m_i}, \qquad i = 1, 2, \ldots, k$$

(системата е разрешима, вследствие на задача 193, тъй като числата $m_1, \ldots, m_k$ са две по две взаимно прости). Нека също $y_0 \in \mathbb{N}$ е решение на системата

$$y \equiv -j \pmod{M_j}, \qquad j = 1, 2, \ldots, k$$

(която е разрешима по аналогична причина). Тогава, ако $1 \leq h, l \leq k$ и ако $p_{h,l}$ е простото число, намиращо се на h–тия ред и l–тия стълб на таблицата, то $p_{h,l} \mid (m_h, M_l)$, следователно $p_{h,l} \mid (x_0 + h, y_0 + l)$, с което твърдението е доказано.

13 Сравнения от по–висока степен.

Задача 199. Нека p е просто число, $n \in \mathbb{N}$ и нека $f \in \mathbb{Z}[x]$ е полином от степен n. Да се докаже, че ако сравнението $f(x) \equiv 0 \pmod{p}$ има повече от n решения, то всички коефициенти на $f(x)$ се делят на p.

Решение: Ще докажем твърдението с индукция по n. Нека $n = 1$ и $f(x) = a_0x + a_1$. Ако $x_1, x_2 \in \mathbb{Z}$, $x_1 \not\equiv x_2 \pmod{p}$ и $a_0x_i + a_1 \equiv 0 \pmod{p}$, $i = 1, 2$, то изваждайки тези срванения, получаваме $p \mid a_0(x_1 - x_2)$ и от задача 44 следва, че $p \mid a_0$. Оттук непосредствено следва, че $p \mid a_1$.

Нека сега $n > 1$ и да допуснем, че сме доказали твърдението за числата $k \in \mathbb{N}$, $k < n$. Нека $f(x)$ е от степен n и нека $x_i \in \mathbb{Z}, 1 \leq i \leq n+1$ са две по две несравними по модул p решения на $f(x) \equiv 0 \pmod{p}$. Представяме полинома във вида

$$f(x) = f(x_{n+1}) + (x - x_{n+1})h(x)\,, \qquad (i)$$

където $h(x) \in \mathbb{Z}[x]$ е от степен $n - 1$. Имаме $p \mid f(x_{n+1})$, а освен това при $1 \leq i \leq n$ е изпълнено

$$0 \equiv f(x_i) = f(x_{n+1}) + (x_i - x_{n+1})h(x_i) \equiv (x_i - x_{n+1})h(x_i) \pmod{p}\,.$$

От задача 44 и от допускането за числата x_i получаваме, че $p \mid h(x_i)$ при $1 \leq i \leq n$, следователно, според индукционното предположение, коефициентите на $h(x)$ се делят на p. Тогава от (i) следва, че същото свойство притежава и $f(x)$.

Забележка: От задача 199 следва, че ако не всички коефициенти на полинома $f(x)$ се делят на простото число p, то броят на решенията на сравнението $f(x) \equiv 0 \pmod{p}$ не надминава степента на $f(x)$. Това е частен случай на малко по–общо твърдение, известно като *теорема на Лагранж*.

Задача 200. Вярно ли е твърдението на задача 199, ако модулът е съставно число?

Отговор: Не е вярно. Например, сравнението $x^2 \equiv 1 \pmod{8}$ има 4 решения.

Задача 201. Нека $p > 2$ е просто число и

$$f(x) = (x-1)(x-2)\dots(x-(p-1)) - x^{p-1} + 1\,.$$

Да се докаже, че всички коефициенти на полинома $f(x)$ се делят на p.

Решение: От задача 175 следва, че всяко от числата $1, 2, \dots, p-1$ е решение на сравнението $f(x) \equiv 0 \pmod{p}$. Тъй като $f(x)$ е от степен $p-2$, то твърдението следва от задача 199.

Задача 202. Да се докаже, че ако p е просто число, то е изпълнено $(p-1)! \equiv -1 \pmod{p}$.

Решение: При $p = 2$ твърдението се проверява непосредствено, а при $p > 2$ е следствие от задача 201, тъй като свободният член на полинома, разглеждан там, е равен на $(p-1)! + 1$.

Забележка: Твърдението от задача 202 е известно като *теорема на Уилсън*.

Задача 203. Да се докаже, че $(m-1)! \not\equiv -1 \pmod{m}$, ако числото $m \in \mathbb{N}$ е съставно.

Упътване: Ако $k \mid m$ и $1 < k < m$, то $k \mid (m-1)!$, следователно $k \nmid (m-1)! + 1$.

Забележка: Задачи 202 и 203 ни дават критерий за простота на естествено число. За съжаление, той на практика е неприложим, тъй като числото $(m-1)!$ е огромно дори и при не много големи m.

Задача 204. Да се докаже, че ако $p > 3$ е просто число, то е в сила $\sum_{k=1}^{p-1} \frac{(p-1)!}{k} \equiv 0 \pmod{p^2}$.

Решение: Да разгледаме полинома $f(x)$, определен в задача 201, и да го запишем във вида

$$f(x) = c_0 x^{p-2} + c_1 x^{p-3} + \dots + c_{p-4} x^2 + c_{p-3} x + c_{p-2}\,. \qquad (i)$$

Ясно е, че $c_{p-3} = -\sum_{k=1}^{p-1} \frac{(p-1)!}{k}$ и $c_{p-2} = (p-1)! + 1$. От определението на $f(x)$ следва, че

$$f(p) = (p-1)! - p^{p-1} + 1 = c_{p-2} - p^{p-1} \equiv c_{p-2} \pmod{p^3}\,. \qquad (ii)$$

От друга страна, от (i) получаваме

$$f(p) \equiv c_{p-4}p^2 + c_{p-3}p + c_{p-2} \pmod{p^3}. \qquad (iii)$$

Като извадим (ii) и (iii), намираме $c_{p-4}p^2 + c_{p-3}p \equiv 0 \pmod{p^3}$ и от задача 159 следва, че $c_{p-4}p + c_{p-3} \equiv 0 \pmod{p^2}$. Но според задача 201 е изпълнено $p \mid c_{p-4}$. Тогава $c_{p-3} \equiv 0 \pmod{p^2}$, което трябваше да се докаже.

Забележка: Твърдението от задача 204 е известно като *теорема на Волстенхолм*.

Задача 205. Нека p е просто число и $f \in \mathbb{Z}[x]$. Да се докаже, че съществува полином $r \in \mathbb{Z}[x]$ от степен по–малка от p и такъв, че сравненията $f(x) \equiv 0 \pmod{p}$ и $r(x) \equiv 0 \pmod{p}$ са еквивалентни.

Упътване: Да се използува задача 175.

Задача 206. Да се сведе сравнението $x^{12} + 6x^9 - x^2 + 2 \equiv 0 \pmod{7}$ до сравнение от по–ниска степен.

Задача 207. Нека p е просто число, $l \in \mathbb{N}$, $l \geq 2$ и $\mathcal{M}$ е п.с.о. $(\mathrm{mod}\ p^l)$. Даден е полиномът $f \in \mathbb{Z}[x]$ от степен $n \geq 1$ и нека $x_0 \in \mathbb{Z}$ е решение на сравнението $f(x) \equiv 0 \pmod{p^{l-1}}$. Да се докажат следните твърдения:

а) Ако $f'(x_0) \not\equiv 0 \pmod{p}$, то съществува единствено $y \in \mathcal{M}$, което удовлетворява условията

$$f(y) \equiv 0 \pmod{p^l}, \qquad y \equiv x_0 \pmod{p^{l-1}}. \qquad (i)$$

б) Ако $f'(x_0) \equiv 0 \pmod{p}$ и $f(x_0) \not\equiv 0 \pmod{p^l}$, то не съществуват $y \in \mathcal{M}$, удовлетворващи (i).

в) Ако $f'(x_0) \equiv 0 \pmod{p}$ и $f(x_0) \equiv 0 \pmod{p^l}$, то съществуват точно p на брой числа $y \in \mathcal{M}$, които удовлетворват (i).

Решение: По формулата на Тейлор имаме

$$f(x+h) = f(x) + \frac{f'(x)}{1!}h + \frac{f''(x)}{2!}h^2 + \cdots + \frac{f^{(n)}(x)}{n!}h^n. \qquad (ii)$$

От задача 82 следва, че $\frac{1}{k!}f^{(k)}(x) \in \mathbb{Z}[x]$ за всяко $k \in \mathbb{N}$. Прилагаме (ii) при $x = x_0$, $h = tp^{l-1}$, където $t \in \mathbb{Z}$. По условие $f(x_0) = mp^{l-1}$ за някое

$m \in \mathbb{Z}$. Следователно, като имаме предвид неравенството $2(l-1) \geq l$, получаваме

$$f(x_0 + tp^{l-1}) \equiv (m + f'(x_0)\, t)\, p^{l-1} \pmod{p^l}\,. \qquad (iii)$$

Да докажем а). Понеже $p \nmid f'(x_0)$, то според задача 186, съществува $t_0 \in \mathbb{Z}$, такова че $m + f'(x_0)\, t_0 \equiv 0 \pmod{p}$. Тогава числото $y_0 \in \mathcal{M}$, за което $y_0 \equiv x_0 + t_0 p^{l-1} \pmod{p}$, удовлетворява (i). Обратно, ако за някое $y \in \mathcal{M}$ са в сила условията (i), то според второто от тях имаме $y = x_0 + tp^{l-1}$, където $t \in \mathbb{Z}$. От първото от условията (i), от (iii) и от задача 159 следва, че $m + f'(x_0)\, t \equiv 0 \pmod{p}$ и като приложим отново задача 186 получаваме $t \equiv t_0 \pmod{p}$. Тогава определение 34 ни дава $y = y_0$, с което а) е доказано.

Да докажем б). Ако има число $y \in \mathcal{M}$, което удовлетворява (i), то $y = x_0 + tp^{l-1}$ за някое $t \in \mathbb{Z}$, но тогава влизаме в противоречие с (iii).

Да разгледаме случая в). Тогава за всяко $t \in \mathbb{Z}$ числото $y = x_0 + tp^{l-1}$ изпълнява условията (i). Остава да приложим задача 168.

Забележка: Последната задача ни дава метод за решаване на сравнения по модул p^l, където p е просто число. Първо се намират решенията на съответното сравнение по модул p (например чрез извършване на всевъзможните проверки). След това всяко от решенията последователно се продължава, ако това е възможно, до едно или повече решения на съответните сравнения по модули $p^2, p^3, \ldots, p^l$.

Задача 208. Нека $f(x) = x^4 - 4x^3 - 8x^2 - 9x - 4$. Да се реши сравнението $f(x) \equiv 0 \pmod{25}$.

Решение: Лесно се проверява, че решенията на $f(x) \equiv 0 \pmod{5}$ са $x \equiv 2 \pmod{5}$ и $x \equiv 3 \pmod{5}$. Имаме $f'(x) = 4x^3 - 12x^2 - 16x - 9$, откъдето $f'(2) \equiv 3 \pmod{5}$ и $f'(3) \equiv 3 \pmod{5}$. От задача 207 следва, че даденото сравнение има две решения.

Да намерим първо решението, за което $x \equiv 2 \pmod{5}$. В този случай имаме $x = 2 + 5t$ за някое $t \in \mathbb{Z}$. Като работим, както при решението на задача 207, получаваме сравнението $f(2) + 5f'(2)t \equiv 0 \pmod{25}$, или все едно $5 + 15t \equiv 0 \pmod{25}$. Тогава $1 + 3t \equiv 0 \pmod{5}$, откъдето получаваме $t \equiv 3 \pmod{5}$. Следователно $x \equiv 17 \pmod{25}$ е първото от решенията на даденото сравнение.

Сега да намерим решението, за което $x \equiv 3 \pmod 5$. Ако $x = 3 + 5t$, където $t \in \mathbb{Z}$, то получаваме последователно $f(3)+5f'(3)t \equiv 0 \pmod{25}$, $20 + 15t \equiv 0 \pmod{25}$, $4 + 3t \equiv 0 \pmod 5$, $t \equiv 2 \pmod 5$. Следователно $x \equiv 13 \pmod{25}$ е второто от решенията на даденото сравнение.

Задача 209. Да се реши сравнението $f(x) \equiv 0 \pmod{49}$ при $f(x) = x^5 + x - 15$.

Упътване: Чрез непосредствена проверка установяваме, че решенията на $f(x) \equiv 0 \pmod 7$ са $x \equiv 3 \pmod 7$ и $x \equiv 5 \pmod 7$. Тъй като $7 \mid f'(3)$ и $49 \nmid f(3)$, то според задача 207 даденото сравнение няма решения измежду числата $x \equiv 3 \pmod 7$. По–нататък, тъй като $7 \nmid f'(5)$, то като работим, както при решението на задача 208, намираме, че решението на даденото сравнение е $x \equiv 47 \pmod{49}$.

Задача 210. Да се решат сравненията

а) $x^4 + 67x - 29 \equiv 0 \pmod{121}$;

б) $x^2 - 54x + 37 \equiv 0 \pmod{169}$;

в) $x^3 - 3x^2 + x + 2 \equiv 0 \pmod{125}$.

Упътване и отговори:

а) Нека $f(x) = x^4 + 67x - 29$ и тогава $f'(x) = 4x^3 + 67$. Решенията на $f(x) \equiv 0 \pmod{11}$ са $x \equiv 2, 3, 4 \pmod{11}$.

Да намерим първо решенията, за които $x \equiv 2 \pmod{11}$. Лесно се проверява, че $11 \mid f'(2)$ и $121 \mid f(2)$. Като работим както при решението на задача 207 в), получаваме, че съответните решения на даденото сравнение са $x \equiv 2 + 11t \pmod{121}$, където $t = 0, 1, 2, \ldots, 10$.

По–нататък, имаме $11 \nmid f'(3)$. Прилагайки метода за решаване на задача 207 а), получаваме едно решение на даденото сравнение, за което $x \equiv 3 \pmod{11}$, а именно $x \equiv 14 \pmod{121}$. Аналогично, $11 \nmid f'(4)$ и има едно решение, за което $x \equiv 4 \pmod{11}$, а именно $x \equiv 92 \pmod{121}$.

Окончателно, всички решения на $f(x) \equiv 0 \pmod{121}$ са

$$x \equiv 2, 13, 14, 24, 35, 46, 57, 68, 79, 90, 92, 101, 112 \pmod{121}.$$

б) $x \equiv 23, 31 \pmod{169}$.

в) $x \equiv 2 \pmod{125}$.

Задача 211. Да се предложи метод за решаване на сравнение от вида

$$f(x) \equiv 0 \pmod{m}, \qquad (i)$$

при $f \in \mathbb{Z}[x]$ когато ни е известно каноничното разлагане на числото $m \in \mathbb{N}$.

Упътване: Нека m има канонично разлагане $m = p_1^{l_1} \dots p_s^{l_s}$. Като използуваме задача 161, свеждаме сравнението (i) до системата от сравнения

$$f(x) \equiv 0 \pmod{p_i^{l_i}}, \qquad 1 \le i \le s. \qquad (ii)$$

Всяко от тези сравнения решаваме по метода, описан в решението на задача 207. Ако някое от сравненията в (ii) няма решение, то (i) също няма решение. Нека сега всички сравнения в (ii) са разрешими и нека решението на i–тото от тях се дава чрез формулата

$$x \equiv c_i^{(1)}, c_i^{(2)}, \dots, c_i^{(\nu_i)} \pmod{p_i^{l_i}}.$$

Вземаме произволен набор от числа $j_1, \dots, j_s \in \mathbb{N}$, такива че

$$1 \le j_1 \le \nu_1, \ \dots, \ 1 \le j_s \le \nu_s \qquad (iii)$$

и образуваме системата

$$x \equiv c_i^{(j_i)} \pmod{p_i^{l_i}}, \qquad 1 \le i \le s.$$

Като я решим по метода, изложен в решението на задача 193, намираме решение на (i). Разглеждайки всевъзможните набори $j_1, \dots, j_s$, които удовлетворяват (iii), получаваме всички решения на (i).

Задача 212. Да се решат сравненията

а) $x^3 - 161x^2 + 191x - 151 \equiv 0 \pmod{360}$;

б) $x^4 + 7x^3 + 4x^2 + 13x + 2 \equiv 0 \pmod{2520}$;

в) $x^2 - 180x + 131 \equiv 0 \pmod{7920}$.

Упътване и отговори: а) Тъй като $360 = 2^3 \cdot 3^2 \cdot 5$, то сравнението е еквивалентно на системата

$$f(x) \equiv 0 \pmod{2^3}, \quad f(x) \equiv 0 \pmod{3^2}, \quad f(x) \equiv 0 \pmod{5},$$

където $f(x) = x^3 - 161x^2 + 191x - 151$. Прилагаме към всяко от сравненията метода от задача 207, след което прилагаме задача 193 и намираме, че даденото сравнение има 48 решения, които се дават с формулата $x \equiv a + 30b \pmod{360}$, където $a = 11, 13, 17$; $b = 0, 1, 2, \ldots, 11$.

б) Имаме $2520 = 2^3 \cdot 3^2 \cdot 5 \cdot 7$ и сравнението няма решение, тъй като е неразрешимо съответното сравнение по модул 5.

в) Сравнението има 32 решения, а именно $x \equiv a + 3960b \pmod{7920}$, където a приема стойности 83, 457, 713, 1073, 1307, 1483, 1667, 1843, 2297, 2473, 2657, 2833, 3067, 3427, 3672, 3683, а b приема стойности $0, 1$.

14 Класически експоненциални суми

Определение 39. За всяко $x \in \mathbb{R}$ полагаме, за простота на записа, $e(x) = e^{2\pi i x}$. Сума от вида $\sum_{a<k\leq b} e\big(f(k)\big)$, където $a, b \in \mathbb{R}$, $a < b$ и където $f(x)$ е дадена реална функция, се нарича *експоненциална сума* или още *тригонометрична сума*.

Задача 213. Да се провери, че

а) За всяко $x \in \mathbb{Z}$ е в сила $e(x) = 1$.

б) За всяко $x \in \mathbb{R}$ е в сила $|e(x)| = 1$.

в) За всеки $x, y \in \mathbb{R}$ е изпълнено $e(x + y) = e(x)\, e(y)$.

г) За всяко $n \in \mathbb{N}$ функцията $e\big(\frac{x}{n}\big)$ е периодична спрямо променливата x и има период n.

Задача 214. Да се докаже, че за всяка експоненциална сума е в сила неравенството

$$\Big| \sum_{a<k\leq b} e\big(f(k)\big) \Big| \leq [b] - [a]\,.$$

Решение: Твърдението следва от неравенството на триъгълника и задача 213 б).

Забележка: Неравенството от задача 214 се нарича *тривиална оценка* за дадената експоненциална сума. Ако редицата от дробните части на числата $f(k)$, където $a < k \leq b$, е *равномерно разпределена* в интервала $[0, 1)$ (тук няма да даваме строга дефиниция на това понятие), то бихме могли да очакваме, че комплексните числа $e(f(k))$ при

събирането си ще се „унищожават“ взаимно. Тогава модулът на експоненциалната сума ще е много по–малък от $[b]-[a]$, т.е. ще е налице *нетривиална оценка* за сумата.

Решаването на много проблеми в теорията на числата се свежда до намирането на нетривиални оценки за експоненциални суми от един или друг вид.

Задача 215. Нека $m \in \mathbb{N}$ и нека $\alpha \in \mathbb{R} \setminus \mathbb{Z}$. Да се докаже, че

$$\sum_{k=1}^{m} e\big(\alpha k\big) = \frac{e(m\alpha)-1}{e(\alpha)-1}\, e(\alpha)\,.$$

Решение: Твърдението се получава непосредствено от правилото за сумиране на членовете на геометрична прогресия.

Забележка: Въпреки своята простота, тъждеството от задача 215 и неговите следствия, изложени в задачи 216 и 217, имат важни приложения.

Оказва се, че и други експоненциални суми, по–сложни от разглежданата в задача 215, могат да бъдат изчислени в явен вид. Такава е, например, сумата на Раманудджан, дефинирана чрез определение 40. Като правило, познаването на точна формула за дадена експоненциална сума има дълбоки и важни аритметични следствия.

Задача 216. Нека $a, m \in \mathbb{N}$. Да се докаже, че

$$\sum_{k=1}^{m} e\Big(\frac{ak}{m}\Big) = \begin{cases} m & \text{ако } m \mid a\,, \\ 0 & \text{ако } m \nmid a\,. \end{cases}$$

Решение: Твърдението следва от задачи 213 а) и 215.

Задача 217. Нека $m \in \mathbb{N}$ и нека $\alpha \in \mathbb{R} \setminus \mathbb{Z}$. Да се докаже, че

$$\Big|\sum_{k=1}^{m} e\big(\alpha k\big)\Big| \leq \min\Big(m, \frac{1}{2||\alpha||}\Big)\,,$$

където $||\alpha||$ означава разстоянието от α до най–близкото цяло число.

Упътване: Да се използуват задача 215 и неравенствата

$$\left|\frac{e(\alpha m)-1}{e(\alpha)-1}\right| \leq \frac{1}{|\sin \pi\alpha|} = \frac{1}{\sin(\pi||\alpha||)} \leq \frac{1}{2||\alpha||}\,.$$

Забележка: Неравенството от задача 217 има смисъл и при $\alpha \in \mathbb{Z}$, стига в този случай да положим $\min\left(m, \frac{1}{2||\alpha||}\right) = m$.

Определение 40. Определяме *функцията на Раманудджан* $c(n,a)$ при $n \in \mathbb{N}$ и $a \in \mathbb{Z}$ посредством формулата

$$c(n,a) = \sum_{\substack{1\leq k\leq n\\(k,n)=1}} e\Big(\frac{ak}{n}\Big)\,.$$

Задача 218. Да се докаже, че сумата на Раманудджан не се променя, ако сумирането се извърши по числа k от произволна р.с.о. $(\mathrm{mod}\ n)$.

Упътване: Да се използува задача 213 г).

Задача 219. Да се докаже, че ако $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$ и $(n,b) = 1$, то $c(n,a) = c(n,ab)$.

Упътване: Да се използува задача 218.

Задача 220. Да се докаже, че ако $n \in \mathbb{N}$, $a \in \mathbb{Z}$ и $(n,a) = 1$, то е изпълнено $c(n,a) = \mu(n)$.

Решение: От задача 219 следва, че е достатъчно да разгледаме случая $a = 1$. Като използуваме определение 25, получаваме

$$c(n,1) = \sum_{\substack{1\leq k\leq n\\(k,n)=1}} e\Big(\frac{k}{n}\Big) = \sum_{1\leq k\leq n} e\Big(\frac{k}{n}\Big) \sum_{d|(k,n)} \mu(d)\,.$$

Сменяме реда на сумирането, използуваме задача 216 и намираме

$$c(n,1) = \sum_{d|n} \mu(d) \sum_{\substack{1\leq k\leq n\\ k\equiv 0 \pmod d}} e\Big(\frac{k}{n}\Big) = \sum_{d|n} \mu(d) \sum_{1\leq l\leq \frac{n}{d}} e\Big(\frac{l}{\frac{n}{d}}\Big) = \mu(n)\,.$$

Задача 221. Да се докаже, че при фиксирано a функцията на Рамануджан е мултипликативна по отношение на n.

Решение: Нека $n_1, n_2 \in \mathbb{N}$ и $(n_1, n_2) = 1$. От задачи 173 и 218 намираме

$$c(n_1 n_2, a) = \sum_{\substack{1 \le k \le n \\ (k, n_1 n_2)=1}} e\Big(\frac{ak}{n_1 n_2}\Big) = \sum_{\substack{1 \le k_1 \le n_1 \\ (k_1, n_1)=1}} \sum_{\substack{1 \le k_2 \le n_2 \\ (k_2, n_2)=1}} e\Big(\frac{a(k_1 n_2 + k_2 n_1)}{n_1 n_2}\Big) =$$

$$= \sum_{\substack{1 \le k_1 \le n_1 \\ (k_1, n_1)=1}} e\Big(\frac{ak_1}{n_1}\Big) \sum_{\substack{1 \le k_2 \le n_2 \\ (k_2, n_2)=1}} e\Big(\frac{ak_2}{n_2}\Big) = c(n_1, a)\, c(n_2, a)\,.$$

Задача 222. Нека p е просто число, $l \in \mathbb{N}$, $a \in \mathbb{Z}$, $a \neq 0$ и $\mathrm{ord}_p a = \nu$. Да се докаже, че

$$c(p^l, a) = \begin{cases} p^l - p^{l-1} & \text{ако } l \le \nu\,, \\ -p^{l-1} & \text{ако } l = \nu + 1\,, \\ 0 & \text{ако } l \ge \nu + 2\,. \end{cases}$$

Упътване: Имайки предвид задача 219, можем да считаме, че $a = p^\nu$. Ако $l \le \nu$, то твърдението следва от задача 130 и определения 28 и 40. Ако пък $l > \nu$, то лесно се вижда, че $c(p^l, p^\nu) = p^\nu\, c(p^{l-\nu}, 1)$ и остава да приложим задачи 111 и 220.

Задача 223. Да се докаже, че при $n \in \mathbb{N}$ и $a \in \mathbb{Z}$ е в сила тъждеството

$$c(n, a) = \frac{\varphi(n)}{\varphi\Big(\frac{n}{(n,a)}\Big)} \mu\Big(\frac{n}{(n,a)}\Big)\,. \qquad (i)$$

Упътване: При $a = 0$ твърдението е тривиално. Нека разгледаме случая $a \neq 0$. Да означим израза от дясната част на (i) чрез $h(n, a)$. Функциите $c(n, a)$ и $h(n, a)$ са мултипликативни по отношение на n вследствие на задачи 20, 99, 110, 129 и 221. Тогава от задача 101 следва, че е достатъчно да се докаже равенството $c(p^l, a) = h(p^l, a)$, когато p е просто число и $l \in \mathbb{N}$. По–нататък, нека $\mathrm{ord}_p a = \nu$. Достатъчно е да се докаже, че $c(p^l, p^\nu) = h(p^l, p^\nu)$, което се проверява непосредствено като се използуват задачи 111, 130 и 222.

Определение 41. Нека $l, n \in \mathbb{N}$ и $a \in \mathbb{Z}$. Определяме *сумите на X. Вайл* $S_l(n,a)$ и $S_l^*(n,a)$ посредством формулите

$$S_l(n,a) = \sum_{1 \le k \le n} e\Big(\frac{ak^l}{n}\Big), \qquad S_l^*(n,a) = \sum_{\substack{1 \le k \le n \\ (k,n)=1}} e\Big(\frac{ak^l}{n}\Big).$$

Забележка 1: При $l = 1$ сумите на X. Вайл съвпадат съответно със сумата от задача 216 и със сумата на Рамануджан, които, както видяхме, са напълно изучени. Изследването на сумите на X. Вайл при $l \ge 2$ е много по–трудно.

Забележка 2: Ако вместо израза ak^l в определението на сумите вземем $f(k)$, където $f \in \mathbb{Z}[x]$, то получаваме по–общи суми, които също се наричат суми на X. Вайл. Ако $f(x)$ е полином от втора степен, то съответните суми са известни като *суми на Гаус* .

Задача 224. Да се докаже, че сумите на X. Вайл не се променят, ако сумирането се извърши по числа k от произволна п.с.о. (mod n) и съответно р.с.о. (mod n).

Задача 225. Да се докаже, че ако $l, n_1, n_2 \in \mathbb{N}$, $a_1, a_2 \in \mathbb{Z}$ и $(n_1, n_2) = 1$, то са в сила тъждествата

а) $S_l(n_1n_2, a_1n_2 + a_2n_1) = S_l(n_1, a_1)\, S_l(n_2, a_2)$.

б) $S_l^*(n_1n_2, a_1n_2 + a_2n_1) = S_l^*(n_1, a_1)\, S_l^*(n_2, a_2)$.

Решение: Да докажем а). Ако $k_1, k_2 \in \mathbb{Z}$, то от биномната формула на Нютон получаваме

$$\begin{aligned}(a_1n_2 + a_2n_1)(k_1n_2 + k_2n_1)^l &\equiv (a_1n_2 + a_2n_1)(k_1^l n_2^l + k_2^l n_1^l) \\ &\equiv a_1 n_2^{l+1} k_1^l + a_2 n_1^{l+1} k_2^l \pmod{n_1n_2}.\end{aligned}$$

Като използуваме определение 41, задачи 165, 166, 213, 224 и последната

формула, намираме, че

$$\begin{aligned} S_l(n_1n_2, a_1n_2 + a_2n_1) &= \sum_{1\le k_1\le n_1}\ \sum_{1\le k_2\le n_2} e\Big(\frac{(a_1n_2 + a_2n_1)(k_1n_2 + k_2n_1)^l}{n_1n_2}\Big) = \\ &= \sum_{1\le k_1\le n_1}\ \sum_{1\le k_2\le n_2} e\Big(\frac{a_1n_2^{l+1}k_1^l + a_2n_1^{l+1}k_2^l}{n_1n_2}\Big) = \\ &= \sum_{1\le k_1\le n_1} e\Big(\frac{a_1(n_2k_1)^l}{n_1}\Big) \sum_{1\le k_2\le n_2} e\Big(\frac{a_2(n_1k_2)^l}{n_2}\Big) = \\ &= S_l(n_1, a_1)\, S_l(n_2, a_2)\,. \end{aligned}$$

Доказателството на б) е аналогично.

Задача 226. Нека $n \in \mathbb{N}$, $a \in \mathbb{Z}$ и $(a, n) = 1$. Да се докаже, че за сумата на Гаус $S = \sum_{1\le k\le n} e\big(\frac{ak^2}{n}\big)$ е в сила оценката

$$|S| \le \begin{cases} \sqrt{n} & \text{ако } 2 \nmid n\,, \\ \sqrt{2n} & \text{ако } 2 \mid n\,. \end{cases}$$

Решение: Имаме $|S|^2 = S\,\overline{S}$ (тук $\overline{S}$ означава комплексно спрегнатото на S). Тогава

$$|S|^2 = \sum_{1\le k_1\le n} e\Big(\frac{ak_1^2}{n}\Big) \sum_{1\le k_2\le n} e\Big(\frac{-ak_2^2}{n}\Big) = \sum_{1\le k_1,k_2\le n} e\Big(\frac{a(k_1^2 - k_2^2)}{n}\Big)\,.$$

Ако $k_1 - k_2 \equiv h \pmod n$ за някое $h \in \mathbb{N}$, то лесно се вижда, че тогава е изпълнено

$$k_1^2 - k_2^2 \equiv h(h + 2k_2) \equiv h^2 + 2hk_2 \pmod n\,,$$

следователно, като приложим задача 213, получаваме

$$e\Big(\frac{a(k_1^2 - k_2^2)}{n}\Big) = e\Big(\frac{ah^2}{n}\Big) \cdot e\Big(\frac{2ahk_2}{n}\Big)\,.$$

Да забележим, че при фиксирани h и k_2 има единствено k_1, такова, че $1 \le k_1 \le n$, $k_1 \equiv k_2 + h \pmod n$. От последните съображения и от

задача 216 получаваме

$$|S|^2 = \sum_{1\le h\le n} \sum_{\substack{1\le k_1,k_2\le n\\ k_2-k_1\equiv h \pmod n}} e\Big(\frac{ah^2}{n}\Big)\cdot e\Big(\frac{2ahk_2}{n}\Big) =$$
$$= \sum_{1\le h\le n} e\Big(\frac{ah^2}{n}\Big) \sum_{1\le k_2\le n} e\Big(\frac{2ahk_2}{n}\Big) =$$
$$= n \sum_{\substack{1\le h\le n\\ 2ah\equiv 0 \pmod n}} e\Big(\frac{ah^2}{n}\Big).$$

Тъй като $(a,n)=1$, то последната сума се състои от две събираеми, ако $2 \mid n$ и само от едно, ако $2 \nmid n$. Следователно

$$|S|^2 \le \begin{cases} n & \text{ако } 2\nmid n\,,\\ 2n & \text{ако } 2\mid n\,, \end{cases}$$

с което твърдението е доказано.

Забележка 1: Методът на решение на задача 226 е илюстрация на метода на X. Вайл за намиране на нетривиални оценки за експоненциални суми. Ако, обаче, степента на полинома в експонентата е висока, то получените оценки са твърде слаби. Много по–точни оценки на експоненциални суми се получават по метод, разработен от Виноградов.

Забележка 2: За сумата на Гаус от задача 226 при $a=1$ е известна точна формула, а именно

$$\sum_{1\le k\le n} e\Big(\frac{k^2}{n}\Big) = \frac{1+i^{-n}}{1+i^{-1}}\sqrt{n} = \begin{cases} (1+i)\sqrt{n} & \text{ако } n\equiv 0 \pmod 4\,,\\ \sqrt{n} & \text{ако } n\equiv 1 \pmod 4\,,\\ 0 & \text{ако } n\equiv 2 \pmod 4\,,\\ i\sqrt{n} & \text{ако } n\equiv 3 \pmod 4\,. \end{cases}$$

Тази формула е получена от Гаус и има важни приложения в теорията на числата.

Определение 42. Нека $n\in\mathbb{N}$. За всяко $k\in\mathbb{Z}$, за което $(k,n)=1$, определяме числото $\overline{(k)}_n \in \mathbb{N}$ посредстом условията $k\overline{(k)}_n \equiv 1 \pmod n$, $1\le \overline{(k)}_n \le n$.

Забележка: Ако стойността на модула n се подразбира от контекста, то за простота пишем $\overline{k}$ вместо $\overline{(k)}_n$. Например, ако $\overline{k}$ участвува в сравнение по модул n се подразбира, че $\overline{k} = \overline{(k)}_n$.

Задача 227. Да се обоснове коректността на определение 42.

Задача 228. Да се докаже, че ако числата k пробягват р.с.о $(\mathrm{mod}\ n)$, то числата $\overline{(k)}_n$ образуват също р.с.о $(\mathrm{mod}\ n)$.

Задача 229. Да се докаже, че ако $n \in \mathbb{N}$, $k \in \mathbb{Z}$ и $(k,n) = 1$, то е изпълнено $\overline{(-k)} \equiv -\overline{k}\ (\mathrm{mod}\ n)$.

Задача 230. Нека $n \in \mathbb{N}$; $k_1, k_2 \in \mathbb{Z}$ като $(n, k_1 k_2) = 1$. Да се докаже, че ако $k_1 \equiv k_2\ (\mathrm{mod}\ n)$, то $\overline{k_1} = \overline{k_2}$.

Задача 231. Нека $n \in \mathbb{N}$; $k_1, k_2 \in \mathbb{Z}$ като $(n, k_1 k_2) = 1$. Да се докаже, че $\overline{(k_1 k_2)} \equiv \overline{k_1}\,\overline{k_2}\ (\mathrm{mod}\ n)$.

Задача 232. Нека $n_1, n_2 \in \mathbb{N}$; $k_1, k_2 \in \mathbb{Z}$, като е изпълнено

$$(n_1, k_1) = (n_2, k_2) = (n_1, n_2) = 1\,.$$

Да се докаже, че

$$\overline{(k_1 n_2 + k_2 n_1)}_{n_1 n_2} \equiv \overline{(k_1\, n_2^2)}_{n_1}\, n_2 \ + \ \overline{(k_2\, n_1^2)}_{n_2}\, n_1 \quad (\mathrm{mod}\ n_1 n_2)\,.$$

Решение: Първо да отбележим, че е изпълнено

$$(k_1 n_2 + k_2 n_1, n_1 n_2) = (k_1 n_2^2, n_1) = (k_2 n_1^2, n_2) = 1\,,$$

тъй че задачата е коректно зададена.

От определение 42 следва, че е достатъчно да докажем сравнението

$$(k_1 n_2 + k_2 n_1)\,\big(\,\overline{(k_1\, n_2^2)}_{n_1}\, n_2 \ + \ \overline{(k_2\, n_1^2)}_{n_2}\, n_1\,\big) \equiv 1 \quad (\mathrm{mod}\ n_1 n_2)\,,$$

а то, по силата на задача 161, ще е вярно, ако са в сила съответните сравнения по модули n_1 и n_2.

По модул n_1, вследствие на определение 42, имаме

$$(k_1 n_2 + k_2 n_1)\big(\overline{(k_1\, n_2^2)}_{n_1} n_2 + \overline{(k_2\, n_1^2)}_{n_2} n_1\big) \equiv (k_1 n_2^2)\,\overline{(k_1 n_2^2)}_{n_1} \equiv 1 \quad (\mathrm{mod}\ n_1)\,.$$

Аналогично проверяваме валидността на съответното сравнение и по модул n_2, с което задачата е решена.

Определение 43. Нека $n \in \mathbb{N}$ и $a, b \in \mathbb{Z}$. Определяме *сумата на Клостерман* чрез формулата

$$K(n; a, b) = \sum_{\substack{1 \le k \le n \\ (n,k)=1}} e\Big(\frac{ak + b\overline{k}}{n}\Big).$$

Забележка 1: В горното определение $\overline{k}$ е съкращение на $\overline{(k)}_n$.

Забележка 2: Сумата на Рамануджан се явява сума на Клостерман от специален вид. По–точно, имаме $c(n, a) = K(n; a, 0)$.

Забележка 3: Сумата на Клостерман има много сложна природа. За нея не е известна точна формула, но пък са намерени някои полезни тъждества, изложени в следващите няколко задачи. Знае се също, че ако $(n, ab) = 1$, то за всяко $\varepsilon \in \mathbb{R}$, $\varepsilon > 0$ съществува величина $C(\varepsilon) > 0$, такава че $|K(n; a, b)| \le C(\varepsilon)\, n^{\frac{1}{2}+\varepsilon}$. Тази нетривиална оценка за сумата на Клостерман е получена от А. Вайл и има важни приложения в теорията на числата.

Задача 233. Да се докаже, че сумата на Клостерман не се променя, ако сумирането се извърши по числа k от произволна р.с.о. $(\mathrm{mod}\ n)$.

Упътване: Да се използват задачи 213 г) и 230.

Задача 234. Да се докаже, че за всички $n \in \mathbb{N}$ и $a, b \in \mathbb{Z}$ сумата на Клостерман $K(n; a, b)$ е реално число.

Упътване: Да се използват задачи 172, 229 и 233 за да се установи, че сумата съвпада с комплексно спрегнатата си величина.

Задача 235. Да се докаже, че ако $n \in \mathbb{N}$ и $a, b \in \mathbb{Z}$, то

$$K(n; a, b) = K(n; b, a).$$

Упътване: Да се използват задачи 228 и 233.

Задача 236. Да се докаже, че ако $n \in \mathbb{N}$, $a, b, l \in \mathbb{Z}$ и $(l, n) = 1$, то е изпълнено

$$K(n; a, bl) = K(n; al, b).$$

Упътване: Да се използуват задачи 172, 231 и 233.

Задача 237. Нека $n_1, n_2 \in \mathbb{N}$, като е изпълнено $(n_1, n_2) = 1$ и нека $a_1, a_2 \in \mathbb{Z}$. Да се докаже тъждеството

$$K(n_1 n_2; a_1 n_2^2 + a_2 n_1^2, 1) = K(n_1; a_1, 1)\, K(n_2; a_2, 1)\,.$$

Решение: От задачи 173 и 233 получаваме

$$K(n_1 n_2; a_1 n_2^2 + a_2 n_1^2, 1) =$$
$$= \sum_{\substack{1 \le k_1 \le n_1 \\ (k_1, n_1)=1}} \sum_{\substack{1 \le k_2 \le n_2 \\ (k_2, n_2)=1}} e\Big(\frac{(a_1 n_2^2 + a_2 n_1^2)(k_1 n_2 + k_2 n_1) + \overline{(k_1 n_2 + k_2 n_1)}_{n_1 n_2}}{n_1 n_2}\Big)\,.$$

Като използуваме сравнението

$$(a_1 n_2^2 + a_2 n_1^2)(k_1 n_2 + k_2 n_1) \equiv k_1 a_1 n_2^3 + k_2 a_2 n_1^3 \pmod{n_1 n_2}$$

и задачи 213 и 232, получаваме

$$K(n_1 n_2; a_1 n_2^2 + a_2 n_1^2, 1) =$$
$$= \sum_{\substack{1 \le k_1 \le n_1 \\ (k_1, n_1)=1}} \sum_{\substack{1 \le k_2 \le n_2 \\ (k_2, n_2)=1}} e\Big(\frac{a_1 k_1 n_2^2 + \overline{(k_1 n_2^2)}_{n_1}}{n_1}\Big)\, e\Big(\frac{a_2 k_2 n_1^2 + \overline{(k_2 n_1^2)}_{n_2}}{n_2}\Big)\,.$$

Вследствие на задачи 172 и 233, последната двойна сума е произведение на две суми на Клостерман, а именно $K(n_i; a_i, 1)$, $i = 1, 2$, с което твърдението е доказано.

15 Елементарни резултати за разпределението на простите числа

Определение 44. За всяко $x \in \mathbb{R}$, $x > 0$, означаваме

$$\pi(x) = \sum_{p \le x} 1\,, \qquad \theta(x) = \sum_{p \le x} \ln p\,, \qquad \psi(x) = \sum_{k \le x} \Lambda(k)\,,$$

където в изразите за $\pi(x)$ и $\theta(x)$ сумирането е по простите числа, които не надминават x, а в определението на $\psi(x)$ чрез $\Lambda(k)$ е означена функцията на Манголд.

Забележка: Функциите $\theta(x)$ и $\psi(x)$ са въведени от Чебишев.

Примери: $\pi(1) = \theta(1,7) = \psi(0,96) = 0$, $\pi(3) = 2$, $\pi(7,2) = 4$, $\theta(6,3) = \ln 2 + \ln 3 + \ln 5$, $\psi(10) = \ln 2 + \ln 3 + \ln 2 + \ln 5 + \ln 7 + \ln 2 + \ln 3$.

Задача 238. Нека $x \in \mathbb{R}$, $x \geq 1$. Полагаме $P = \prod_{p \leq \sqrt{x}} p$, ако $x \geq 4$ и $P = 1$, ако $x \in [1,4)$. Да се докаже тъждеството

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

Решение: Твърдението се проверява непосредствено, ако $x \in [1,4)$. Да разгледаме случая $x \geq 4$. Нека означим с S броя на числата $n \in \mathbb{N}$, $n \leq x$, за които $(n,P) = 1$. Като използуваме определение 25 и задача 77, получаваме

$$S = \sum_{n \leq x} \sum_{d|(n,P)} \mu(d) = \sum_{d|P} \mu(d) \sum_{\substack{n \leq x \\ n \equiv 0 \pmod d}} 1 = \sum_{d|P} \mu(d) \left[\frac{x}{d}\right].$$

От друга страна, от задача 40 виждаме, че числото $n \in \mathbb{N}$, $n \leq x$, е взаимно просто с P, точно когато n е просто число от интервала $(\sqrt{x}, x]$, или пък ако $n = 1$. Следователно $S = \pi(x) - \pi(\sqrt{x}) + 1$, с което твърдението е доказано.

Забележка 1: Бихме могли да се опитаме да извлечем полезна информация от формулата за $\pi(x)$ от задача 238. За малки стойности на x това не е трудно, но за големи е принципно невъзможно, тъй като величината P расте изключително бързо с нарастването на x.

Забележка 2: Доказателството на тъждеството от задача 238 представлява, по същество, приложение на така нареченото *решето на Ератостен*. През 20–ти век методите на решетото са разработени и приложени към най–разнообразни задачи от теорията на числата от Брун, Селберг и други математици.

Теорема на Чебишев. Съществуват константи $c_1 > 0$, $c_1' > 0$, $x_1 \geq 2$, такива че при $x \geq x_1$ е изпълнено

$$c_1 \frac{x}{\ln x} \leq \pi(x) \leq c_1' \frac{x}{\ln x}.$$

Забележка: Чебишев е доказал горните оценки с конкретни стойности за константите c_1 и c_1', намиращи се твърде близо до 1. В следващите задачи ще изложим опростен вариант на метода на Чебишев и ще получим по–груби оценки за c_1 и c_1'. Намиране на точни оценки за тези константи е трудна задача. Да отбележим, че горната оценка за $\pi(x)$ може да бъде доказана с константи c_1 и c_1', които се намират произволно близо до единица, а именно изпълнено е

$$\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\ln x}} = 1\,. \qquad (i)$$

Тази формула е известна под името *асимптотичен закон за разпределение на простите числа* и доказана през 1896 г. независимо от Адамар и Вале–Пусен.

Да отбележим, че функцията $\pi(x)$ се приближава много по–точно чрез интеграла $\int_2^x \frac{dt}{\ln t}$, отколкото чрез функцията $\frac{x}{\ln x}$.

Адамар и Вале–Пусен са доказали, че

$$\pi(x) = \int_2^x \frac{dt}{\ln t} + \Delta(x)\,, \qquad (ii)$$

като за остатъчния член $\Delta(x)$ е в сила оценката

$$\Delta(x) = \mathcal{O}\big(\, x\, e^{-c\,\sqrt{\ln x}}\,\big) \qquad (iii)$$

за някаква константа $c > 0$. Не е трудно да се провери, че

$$\lim_{x\to\infty} \frac{\int_2^x \frac{dt}{\ln t}}{\frac{x}{\ln x}} = 1\,,$$

така че от (ii) и (iii) следва (i). Най–добрата оценка за $\Delta(x)$ е получена от Виноградов, който е установил, че

$$\Delta(x) = \mathcal{O}\Big(x\, e^{-c\,(\ln x)^{3/5}\,(\ln\ln x)^{-1/5}}\Big) \qquad (iv)$$

за някаква константа $c > 0$.

Да отбележим, че от хипотезата на Риман би следвала оценката

$$\Delta(x) = \mathcal{O}\big(\sqrt{x}\,\ln^2 x\big)\,,$$

която е несравнимо по–силна от (iii) и (iv).

Задача 239. Да се докаже, че теоремата на Чебишев е еквивалентна на следното твърдение:

Съществуват константи $c_2 > 0, c_2' > 0, x_2 \geq 2$ такива, че при $x \geq x_2$ е изпълнено

$$c_2 x \leq \theta(x) \leq c_2' x\,.$$

Решение: Очевидно имаме

$$\theta(x) \leq \pi(x) \ln x\,.$$

От друга страна

$$\theta(x) \geq \sum_{\sqrt{x}<p\leq x} \ln p \geq \big(\pi(x) - \pi(\sqrt{x})\big) \ln \sqrt{x} = \frac{1}{2}\pi(x) \ln x + \mathcal{O}(\sqrt{x} \ln x)\,.$$

От горните оценки твърдението следва непосредствено.

Задача 240. Да се докаже, че за всяко $n \in \mathbb{N}$, $n \geq 2$ е в сила неравенството

$$\prod_{p\leq n} p \leq 4^n\,.$$

Решение: Ще докажем твърдението чрез индукция по n. При $n = 2$ твърдението се проверява непосредствено

Нека $n \geq 3$ и нека допуснем, че твърдението е вярно за всички $m \in \mathbb{N}$, такива че $2 \leq m < n$. Ако n е четно, то като използуваме индукционното допускане, получаваме

$$\prod_{p\leq n} p = \prod_{p\leq n-1} p \leq 4^{n-1} < 4^n\,.$$

Сега да допуснем, че n е нечетно и да положим $n = 2m + 1$. Да разгледаме биномния коефициент

$$M = \binom{2m+1}{m} = \frac{(2m+1)(2m)(2m-1)\ldots(m+2)}{m!}\,.$$

Като използуваме, че $2^{2m+1} = (1+1)^{2m+1} \geq 2M$, получаваме $M \leq 4^m$. По–нататък, да разгледаме числото

$$N = \prod_{m+1<p\leq 2m+1} p\,.$$

Очевидно $N \mid (2m+1)(2m)(2m-1)\ldots(m+2)$ и тъй като $(N, m!) = 1$, то според задача 9 имаме $N \mid M$. Тогава

$$N \leq M \leq 4^m \, .$$

Като използуваме последното неравенство и индукционното предположение, получаваме

$$\prod_{p \leq 2m+1} p = N \prod_{p \leq m+1} p \leq 4^m \, 4^{m+1} \leq 4^{2m+1} \, ,$$

с което твърдението е доказано.

Задача 241. Да се докаже, че при $x \in \mathbb{R}$, $x \geq 1$ е изпълнено

$$\theta(x) \leq x \ln 4 \, .$$

Решение: Твърдението следва директно от задача 240.

Задача 242. Да се докаже, че при $x \in \mathbb{R}$, $x \geq 1$ е изпълнено

$$\psi(x) = \theta(x) + \theta(\sqrt{x}) + \theta(\sqrt[3]{x}) + \ldots \, ,$$

като в последната сума има не повече от $\log_2 x$ събираеми.

Решение: Равенството следва от определението на функциите на Чебишев и от задача 123. По–нататък, ако за някое $k \in \mathbb{N}$ имаме $\theta(\sqrt[k]{x}) \neq 0$, то $\sqrt[k]{x} \geq 2$, следователно $k \leq \log_2 x$.

Задача 243. Да се докаже, че при $x \in \mathbb{R}$, $x \geq 2$ е в сила асимптотичната формула

$$\psi(x) = \theta(x) + \mathcal{O}(\sqrt{x}) \, .$$

Решение: Използуваме задача 242 и получаваме

$$0 \leq \psi(x) - \theta(x) = \theta(\sqrt{x}) + \theta(\sqrt[3]{x}) + \ldots \, .$$

Според задача 241 първото събираемо от дясната страна е равно на $\mathcal{O}(\sqrt{x})$. Останалите събираеми са на брой не повече от $\log_2 x$ и всяко от тях е равно на $\mathcal{O}(\sqrt[3]{x})$.

Задача 244. Да се докаже, че теоремата на Чебишев е еквивалентна на следното твърдение:

Съществуват константи $c_3 > 0, c_3' > 0, x_3 \geq 2$ такива, че при $x \geq x_3$ е изпълнено

$$c_3 x \leq \psi(x) \leq c_3' x\,.$$

Решение: Доказателството следва от задачи 239 и 243.

Задача 245. Да се докаже, че при $x \in \mathbb{R}, x \geq 2$ е в сила оценката

$$\psi(x) = \mathcal{O}(x)\,.$$

Решение: Твърдението следва от задачи 241 и 243.

Задача 246. Да се докаже, че при $x \in \mathbb{R}, x \geq 2$ е в сила асимптотичната формула

$$\sum_{k \leq x} \frac{\Lambda(k)}{k} = \ln x + \mathcal{O}(1)\,.$$

Решение: Използуваме задачи 125, 241 и определение 44 и получаваме

$$\begin{aligned} x \ln x + \mathcal{O}(x) &= \sum_{k \leq x} \Lambda(k) \left[\frac{x}{k}\right] = \sum_{k \leq x} \Lambda(k) \left(\frac{x}{k} - \left\{\frac{x}{k}\right\}\right) = \\ &= x \sum_{k \leq x} \frac{\Lambda(k)}{k} + \mathcal{O}(\psi(x)) = \\ &= x \sum_{k \leq x} \frac{\Lambda(k)}{k} + \mathcal{O}(x)\,. \end{aligned}$$

Остава да разделим полученото равенство на x.

Задача 247. Да се докаже, че при $x \in \mathbb{R}, x \geq 2$ е в сила асимптотичната формула

$$\sum_{p \leq x} \frac{\ln p}{p} = \ln x + \mathcal{O}(1)\,.$$

Решение: Използуваме равенството

$$\sum_{k \leq x} \frac{\Lambda(k)}{k} = \sum_{p \leq x} \frac{\ln p}{p} + \Delta(x)\,,$$

където

$$\Delta(x) = \sum_{\substack{k\geq 2,\, p\\ p^k\leq x}} \frac{\ln p}{p^k} \leq \sum_{p\leq x} \Big(\frac{1}{p^2} + \frac{1}{p^3} + \ldots\Big)\, \ln p \,=$$

$$= \sum_{p\leq x} \frac{\ln p}{p(p-1)} \leq \sum_{k=2}^{\infty} \frac{\ln k}{k(k-1)}\,.$$

Тъй като последният ред е сходящ, имаме $\Delta(x) = \mathcal{O}(1)$. Остава да приложим задача 246 и твърдението е доказано.

Задача 248. Да се докаже, че при $x \in \mathbb{R}$, $x \geq 2$ е в сила асимптотичната формула

$$\sum_{p\leq x} \frac{1}{p} = \ln\ln x + c + \mathcal{O}\Big(\frac{1}{\ln x}\Big),$$

където c е константа.

Упътване: Полагаме

$$f(t) = (\ln t)^{-1}\,, \qquad c_n = \begin{cases} n^{-1}\ln n & \text{ако } n \text{ е просто число}\,,\\ 0 & \text{ако } n \text{ е съставно}\,,\end{cases}$$

след което прилагаме задачи 90 и 247.

Задача 249. Да се намери асимптотична формула за сумата $\sum_{pq\leq x} \frac{1}{pq}$ (сумирането е по всички двойки прости числа p, q, за които $pq \leq x$).

Упътване: Да се представи сумата във вида

$$\sum_{pq\leq x} \frac{1}{pq} = 2\sum_{p\leq\sqrt{x}}\ \sum_{q\leq\frac{x}{p}} \frac{1}{pq} - \sum_{p,\,q\leq\sqrt{x}} \frac{1}{pq}\,,$$

след което да се приложи задача 248.

Задача 250. Да се докаже, че при $x \in \mathbb{R}$, $x \geq 2$ е в сила асимптотичната формула

$$\prod_{p\leq x} \Big(1 - \frac{1}{p}\Big) = \frac{c}{\ln x}\,\Big(1 + \mathcal{O}\Big(\frac{1}{\ln x}\Big)\Big)\,,$$

където $c > 0$ е константа.

Упътване: Произведението да се логаритмува, след което да се приложат формулата на Тейлор и задача 248.

Забележка: Може да се докаже, че константата c от формулата в последната задача е равна на $e^{-\gamma}$, където γ е константата на Ойлер.

Задача 251. Да се докаже, че съществува константа $c > 0$, такава че при всяко $x \in \mathbb{R}$, $x \geq 2$ е изпълнено

$$\theta(x) \geq c\,x\,. \qquad (i)$$

Решение: Нека $c_0 > 0$ е константата, включена в събираемото $\mathcal{O}(1)$ от формулата на задача 247, или нека имаме

$$\Big|\sum_{p\leq t}\frac{\ln p}{p} - \ln t\Big| \leq c_0 \quad \text{при} \quad t \geq 2\,. \qquad (ii)$$

Избираме константа $\alpha \in \mathbb{R}$, $0 < \alpha < 1$, така че

$$\ln\frac{1}{\alpha} > 3c_0\,. \qquad (iii)$$

При $x \in \mathbb{R}$, $x \geq 2\alpha^{-1}$ разглеждаме сумата

$$S = \sum_{\alpha x < p \leq x}\frac{\ln p}{p}\,.$$

Като използуваме (ii) намираме, че

$$\Big|S - \ln\frac{1}{\alpha}\Big| \leq 2c_0$$

и тогава от (iii) следва, че $S \geq c_0$. Оттук получаваме

$$c_0 \leq S \leq \frac{1}{\alpha x}\sum_{\alpha x < p \leq x}\ln p \leq \frac{\theta(x)}{\alpha x}\,.$$

Тогава при $x \geq 2\alpha^{-1}$ имаме $\theta(x) \geq c_0\alpha\,x$. Разглеждаме константата $c_1 = \min_{2\leq x\leq 2\alpha^{-1}}\frac{\theta(x)}{x}$ и нека $c = \min(c_0\alpha, c_1)$. Тогава $c > 0$ и освен това неравенството (i) е изпълнено при всяко $x \geq 2$.

Задача 252. Да се докаже теоремата на Чебишев.

Решение: Доказателството следва от задачи 239, 241 и 251.

Забележка: Твърдението на задача 251, а оттам и оценката отдолу за $\pi(x)$ в теоремата на Чебишев, може да бъде получено и по друг начин. В следващите три задачи е изложен един принципно различен метод, предложен от Неир.

Задача 253. Нека $n \in \mathbb{N}$, $n \geq 2$ и $d_n = [1, 2, 3, \ldots, n]$. Да се докаже неравенството

$$d_n \leq n^{\pi(n)} .$$

Решение: Нека p е просто число, $p \leq n$ и нека $\nu_{p,n} = \mathrm{ord}_p(d_n)$. От задача 52 получаваме, че съществува $m \in \mathbb{N}$, $m \leq n$ такова, че $\nu_{p,n} = \mathrm{ord}_p m$. Тогава имаме $p^{\nu_{p,n}} \leq m \leq n$, откъдето

$$d_n = \prod_{p \leq n} p^{\nu_{p,n}} \leq \prod_{p \leq n} n = n^{\pi(n)} .$$

Задача 254. Да се докаже, че ако $n \in \mathbb{N}$, $n \geq 6$ и ако d_n е определено в задача 253, то е в сила неравенството

$$d_n \geq 2^{n-2} .$$

Решение: При $m \in \mathbb{N}$, $m \leq n$ разглеждаме интеграла

$$I_{m,n} = \int_0^1 x^{m-1}(1-x)^{n-m}\, dx .$$

Имаме

$$\begin{aligned} I_{m,n} &= \int_0^1 x^{m-1} \sum_{k=0}^{n-m} \binom{n-m}{k} (-1)^k\, x^k\, dx \;= \\ &= \sum_{k=0}^{n-m} \binom{n-m}{k} (-1)^k \int_0^1 x^{m+k-1}\, dx \;= \\ &= \sum_{k=0}^{n-m} \binom{n-m}{k} (-1)^k\, \frac{1}{m+k} . \end{aligned}$$

Като приведем последната сума от дроби под най–малък общ знаменател и използуваме определението на d_n, получаваме, че

$$I_{m,n} = \frac{a}{d_n} \quad \text{за някое} \quad a \in \mathbb{Z}\,. \tag{i}$$

По–нататък, да разгледаме интеграла

$$J_n(y) = \int_0^1 (1 - x + xy)^{n-1}\, dx\,.$$

Имаме

$$\begin{aligned} J_n(y) &= \int_0^1 \sum_{k=0}^{n-1} \binom{n-1}{k} (xy)^k (1-x)^{n-1-k}\, dx \;= \\ &= \sum_{k=0}^{n-1} \binom{n-1}{k} y^k \int_0^1 x^k (1-x)^{n-1-k}\, dx \;= \\ &= \sum_{k=0}^{n-1} \binom{n-1}{k} I_{k+1,n}\, y^k\,. \end{aligned}$$

От друга страна, след смяна на променливата $u = 1 + (y-1)x$ получаваме, че при $y \neq 1$ е изпълнено

$$J_n(y) = \frac{1}{y-1} \int_1^y u^{n-1}\, du = \frac{y^n - 1}{y-1}\,\frac{1}{n} = \frac{1}{n} \sum_{k=0}^{n-1} y^k\,.$$

Приравняваме коефициентите пред еднаквите степени на y в двете развития на $J_n(y)$ и получаваме

$$I_{m,n} = \frac{1}{n\binom{n-1}{m-1}} = \frac{1}{m\binom{n}{m}} \quad \text{при} \quad m \in \mathbb{N}, \quad m \leq n\,. \tag{ii}$$

От (i) и (ii) следва, че при $m \in \mathbb{N}$, $m \leq n$ е изпълнено

$$d_n \geq m \binom{n}{m}\,. \tag{iii}$$

Измежду всички биномни коефициенти $\binom{n}{m}$ най–голям е този, за който $m = [n/2]$. За него е изпълнено

$$(n+1)\binom{n}{[n/2]} \geq \sum_{k=0}^{n}\binom{n}{k} = 2^n\,,$$

следователно

$$\binom{n}{[n/2]} \geq \frac{2^n}{n+1}\,.$$

Прилагаме неравенството (iii) при $m = [n/2]$ и получаваме

$$d_n \geq [n/2]\binom{n}{[n/2]} \geq \left(\frac{n}{2}-1\right)\frac{2^n}{n+1} \geq 2^{n-2}\,.$$

Задача 255. Да се докаже, че съществуват константи $c > 0$ и $x_0 \geq 2$, такива че при $x \geq x_0$ да е изпълнено

$$\pi(x) \geq c\,\frac{x}{\ln x}\,.$$

Решение: Ако $n \in \mathbb{N}$, $n \geq 6$, то от задачи 253 и 254 следва, че

$$\pi(n) \geq \frac{\ln d_n}{\ln n} \geq \frac{\ln 2^{n-2}}{\ln n} = \frac{(n-2)\ln 2}{\ln n} \geq \frac{\ln 2}{2}\,\frac{n}{\ln n}\,.$$

Тогава, ако $x \in \mathbb{R}$, $x \geq 6$ имаме

$$\pi(x) = \pi([x]) \geq \frac{\ln 2}{2}\,\frac{[x]}{\ln[x]} \geq \frac{\ln 2}{2}\,\frac{x-1}{\ln x} \geq \frac{\ln 2}{4}\,\frac{x}{\ln x}\,.$$

Задача 256. Нека p_n е n–тото просто число. Да се докаже, че съществуват константи $c > 0$, $c' > 0$ и n_0, за които е изпълнено

$$c\,n\ln n \leq p_n \leq c'\,n\ln n \qquad \text{при} \qquad n \geq n_0\,.$$

Решение: Ясно е, че $n \leq p_n$. Като използуваме оценката отгоре за $\pi(x)$ от теоремата на Чебишев, получаваме, че при достатъчно големи n е изпълнено

$$n = \pi(p_n) \leq c_1'\,\frac{p_n}{\ln p_n} \leq c_1'\,\frac{p_n}{\ln n}\,,$$

откъдето следва, че

$$(c_1')^{-1} n \ln n \leq p_n \,.$$

По–нататък, като използуваме оценката отдолу за $\pi(x)$ и очевидния факт $\lim_{n\to\infty} p_n = \infty$, получаваме, че при достатъчно големи n е изпълнено

$$n = \pi(p_n) \geq c_1 \frac{p_n}{\ln p_n} \geq \sqrt{p_n} \,.$$

Оттук $p_n \leq n^2$, следователно при достатъчно големи n имаме

$$n = \pi(p_n) \geq c_1 \frac{p_n}{\ln p_n} \geq \frac{c_1}{2} \frac{p_n}{\ln n} \,.$$

Тогава

$$p_n \leq 2c_1^{-1} n \ln n \,,$$

с което твърдението е доказано.

Задача 257. Да се докаже, че съществува константа $c > 0$, такава че за всяко $n \in \mathbb{N}$ е изпълнено неравенството

$$\varphi(n) \geq \frac{c\, n}{\ln\ln(10n)} \,.$$

Решение: Можем да считаме, че $n > 1$. Нека $n = q_1^{l_1} q_1^{l_2} \ldots q_s^{l_s}$ е каноничното разлагане на n, където $l_i \in \mathbb{N}$ и $q_1 < q_2 < \cdots < q_s$. Първо да забележим, че $n \geq q_1 q_2 \ldots q_s \geq 2^s$, следователно

$$s = \mathcal{O}\big(\ln(10n)\big) \,. \qquad (i)$$

Ако $p_1 < p_2 < \cdots < p_s$ са първите s на брой прости числа, то $p_i \leq q_i$ при $i = 1, 2, \ldots, s$. Оттук и от задача 130 получаваме

$$\frac{n}{\varphi(n)} = \prod_{i=1}^{s} \Big(1 - \frac{1}{q_i}\Big)^{-1} \leq \prod_{i=1}^{s} \Big(1 - \frac{1}{p_i}\Big)^{-1} = \prod_{p\leq p_s} \Big(1 - \frac{1}{p}\Big)^{-1} \,.$$

Тогава от задачи 250, 256 и от оценката (i) следва, че

$$\frac{n}{\varphi(n)} = \mathcal{O}(\ln p_s) = \mathcal{O}(\ln s) = \mathcal{O}(\ln\ln(10n)) \,,$$

с което твърдението е доказано.

Задача 258. Да се докаже, че съществува константа $c > 0$, такава че за всяко $n \in \mathbb{N}$ е изпълнено неравенството

$$\sigma(n) \leq c\, n\, \ln\ln(10n) \,.$$

Упътване: Да се използуват задачи 146 и 257.

16 Средни стойности на числови функции

Задача 259. Да се докаже, че при $x \in \mathbb{R}$, $x \geq 2$ е в сила асимптотичната формула

$$\sum_{n \leq x} \frac{\varphi(n)}{n} = cx + \mathcal{O}(\ln x)\,,$$

където $c = \zeta(2)^{-1}$.

Решение: Използувайки определение 15 и задачи 77, 126, получаваме

$$\sum_{n \leq x} \frac{\varphi(n)}{n} = \sum_{n \leq x} \sum_{d|n} \frac{\mu(d)}{d} = \sum_{d|n} \frac{\mu(d)}{d} \sum_{\substack{n \leq x \\ n \equiv 0 \pmod d}} 1 =$$

$$= \sum_{d \leq x} \frac{\mu(d)}{d} \left[\frac{x}{d}\right] = \sum_{d \leq x} \frac{\mu(d)}{d} \left(\frac{x}{d} - \left\{\frac{x}{d}\right\}\right) = xS_1 - S_2\,, \qquad (i)$$

където

$$S_1 = \sum_{d \leq x} \frac{\mu(d)}{d^2}\,, \qquad S_2 = \sum_{d \leq x} \frac{\mu(d)}{d} \left\{\frac{x}{d}\right\}.$$

Очевидно $|S_2| \leq \sum_{d \leq x} \frac{1}{d}$ и тогава от задача 91 следва, че

$$S_2 = \mathcal{O}(\ln x)\,. \qquad (ii)$$

По–нататък, от задача 150 следва, че

$$S_1 = \zeta(2)^{-1} - S_1'\,, \qquad (iii)$$

където

$$S_1' = \sum_{d > x} \frac{\mu(d)}{d^2}\,.$$

Ясно е, че $|S_1'| \leq \sum_{d > x} \frac{1}{d^2}$ и от задача 95 б) получаваме

$$S_1' = \mathcal{O}\left(\frac{1}{x}\right). \qquad (iv)$$

Твърдението на задачата е следствие от (i) – (iv).

Забележка: Имайки предвид забележката след задача 149, виждаме, че константата от задача 259 е равна на $6\pi^{-2}$.

Задача 260. Да се докаже, че при $x \in \mathbb{R}$, $x \geq 2$ е в сила асимптотичната формула

$$\sum_{n \leq x} \varphi(n) = cx^2 + \mathcal{O}(x \ln x)\,,$$

където $c = \frac{1}{2}\zeta(2)^{-1}$.

Упътване: Да се използува метода от задача 259, или пък да се използува резултата от същата задача и да се приложи тъждеството от задача 90 при $c_n = \frac{\varphi(n)}{n}$ и $f(t) = t$.

Задача 261. Да се докаже, че при $x \in \mathbb{R}$, $x \geq 2$ е в сила

$$\sum_{n \leq x} \frac{n}{\varphi(n)} = cx + \mathcal{O}(x^{\varepsilon})\,,$$

където $c = \sum_{k=1}^{\infty} \frac{\mu^2(k)}{k\varphi(k)}$ и където $\varepsilon \in \mathbb{R}$, $\varepsilon > 0$ е произволно малко, а константата в знака $\mathcal{O}$ зависи от ε.

Решение: Като използуваме задачи 77 и 132, получаваме

$$\sum_{n \leq x} \frac{n}{\varphi(n)} = \sum_{n \leq x} \sum_{d \mid n} \frac{\mu^2(d)}{\varphi(d)} = \sum_{d \leq x} \frac{\mu^2(d)}{\varphi(d)} \left[\frac{x}{d}\right] =$$

$$= \sum_{d \leq x} \frac{\mu^2(d)}{\varphi(d)} \left(\frac{x}{d} - \left\{\frac{x}{d}\right\}\right) = xS_1 + \mathcal{O}(S_2)\,, \qquad (i)$$

където

$$S_1 = \sum_{d \leq x} \frac{\mu^2(d)}{d\varphi(d)}\,, \qquad S_2 = \sum_{d \leq x} \frac{1}{\varphi(d)}\,.$$

От задачи 95 а) и 257 следва, че

$$S_2 = \mathcal{O}\Big(\sum_{d \leq x} \frac{1}{d^{1-\varepsilon}}\Big) = \mathcal{O}(x^{\varepsilon})\,. \qquad (ii)$$

Да разгледаме S_1. Представяме тази сума във вида

$$S_1 = c + \mathcal{O}\big(S_3\big)\,, \qquad (iii)$$

където $S_3 = \sum_{d>x} \frac{1}{d\varphi(d)}$ и където c е константата от условието на задачата (да забележим, че редът, който я представя, е сходящ вследстие на задача 257). Като приложим задачи 95 б) и 257, получаваме

$$S_3 = \mathcal{O}\Big(\sum_{d>x} \frac{1}{d^{2-\varepsilon}}\Big) = \mathcal{O}(x^{-1+\varepsilon})\,. \qquad (iv)$$

Твърдението на задачата следва от (i) – (iv).

Задача 262. Да се докаже, че при $x \in \mathbb{R}$, $x \geq 2$ е в сила асимптотичната формула

$$\sum_{n\leq x} \frac{1}{\varphi(n)} = c \ln x + c' + \mathcal{O}\big(x^{-1+\varepsilon}\big)\,,$$

където $c, c' \in \mathbb{R}$ са константи (c е същата както в задача 261), $\varepsilon \in \mathbb{R}$, $\varepsilon > 0$ и е произволно малко, а константата в знака $\mathcal{O}$ зависи от ε.

Упътване: Да се използуват задачи 90 и 261.

Задача 263. Нека $x \in \mathbb{R}$, $x \geq 2$.

а) Да се докаже, че

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

където величината $\mathcal{L}(x)$ е определена в задача 73.

б) Да се докаже асимптотичната формула

$$\sum_{n\leq x} \tau(n) = x \ln x + (2\gamma - 1)x + \mathcal{O}\big(\sqrt{x}\,\big)\,.$$

Решение: Имаме

$$\mathcal{L}(x) = \sum_{km\leq x} 1 = \sum_{n\leq x} \sum_{km=n} = \sum_{n\leq x} \tau(n)\,,$$

с което а) е доказано. За доказателството на б) остава да използуваме задача 92.

Задача 264. Да се докаже, че при $x \in \mathbb{R}$, $x \geq 2$ е в сила асимптотичната формула

$$\sum_{n \leq x} \frac{\tau(n)}{n} = \frac{1}{2} \ln^2 x + 2\gamma \ln x + c + \mathcal{O}\left(x^{-\frac{1}{2}}\right),$$

където c е константа и γ е константата на Ойлер.

Упътване: Да се използуват задачи 90 и 263 б).

Задача 265. Да се докаже, че за всяко $l \in \mathbb{N}$ може да се намери $c_l > 0$, такова че при всяко $x \in \mathbb{R}$, $x \geq 2$ да е изпълнено

$$\sum_{n \leq x} \frac{\tau(n)^l}{n} \leq c_l \left(\ln x\right)^{2^l}.$$

Решение: При $l = 1$ твърдението следва от задача 264. Да допуснем, че за някое $l \in \mathbb{N}$ константа c_l с даденото свойство съществува. Тогава като използуваме определение 29 и задача 135, получаваме

$$\sum_{n \leq x} \frac{\tau(n)^{l+1}}{n} = \sum_{n \leq x} \frac{\tau(n)^l}{n} \tau(n) = \sum_{n \leq x} \frac{\tau(n)^l}{n} \sum_{km = n} 1 = \sum_{km \leq x} \frac{\tau(km)^l}{km} \leq$$

$$\leq \sum_{k \leq x} \sum_{m \leq x} \frac{\tau(k)^l \, \tau(m)^l}{km} = \left(\sum_{k \leq x} \frac{\tau(k)^l}{k} \right)^2 \leq$$

$$\leq {c_l}^2 \left(\ln x\right)^{2^{l+1}},$$

с което твърдението е доказано.

Задача 266. Да се докаже, че за всяко $l \in \mathbb{N}$ може да се намери $c_l > 0$, такова че при всяко $x \in \mathbb{R}$, $x \geq 2$ да е изпълнено

$$\sum_{n \leq x} \tau(n)^l \leq c_l \, x \left(\ln x\right)^{2^l - 1}.$$

Упътване: При $l = 1$ оценката е следствие от задача 263. Допускаме, че твърдението е вярно за някое $l \in \mathbb{N}$. Тогава като използуваме определение 29 и задача 135, получаваме

$$\sum_{n\leq x} \tau(n)^{l+1} = \sum_{n\leq x} \tau(n)^l \tau(n) = \sum_{n\leq x} \tau(n)^l \sum_{km=n} 1 = \sum_{km\leq x} \tau(km)^l \leq$$

$$\leq \sum_{km\leq x} \tau(k)^l \tau(m)^l \leq \sum_{k\leq x} \tau(k)^l \sum_{m\leq \frac{2x}{k}} \tau(m)^l .$$

В последния израз оценяваме вътрешната сума с помощта на индукционното предположение, а след това прилагаме задача 265.

Задача 267. Да се докаже, че при $x \in \mathbb{R}$, $x \geq 2$ е в сила асимптотичната формула

$$\sum_{n\leq x} \sigma(n) = cx^2 + \mathcal{O}(x \ln x) ,$$

където $c = \frac{1}{2}\zeta(2)$.

Решение: Да забележим, че ако $n \in \mathbb{N}$ и ако d пробягва положителните делители на n, то същото множество пробягва $\frac{n}{d}$. Тогава

$$\sum_{n\leq x} \sigma(n) = \sum_{n\leq x} \sum_{d|n} \frac{n}{d} = \sum_{d\leq x} \sum_{\substack{n\leq x \\ n\equiv 0 \pmod d}} \frac{n}{d} = \sum_{d\leq x} \sum_{k\leq \frac{x}{d}} k .$$

От елементарното тъждество $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$ и от свойствата на функцията $[x]$ получаваме

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

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

Остатъчният член в горната формула е равен на $\mathcal{O}(x \ln x)$ вледствие на задача 91. По–нататък, използуваме задача 95 б) и определение 32 и установяваме, че

$$\sum_{d\leq x} \frac{1}{d^2} = \zeta(2) + \mathcal{O}\left(\frac{1}{x}\right) ,$$

с което твърдението е доказано.

Задача 268. Да се докаже неравенството

$$\sum_{n\leq x} \tau_k(n) \leq \frac{1}{(k-1)!}\, x\, (\ln x + k - 1)^{k-1}\,.$$

Упътване: Да се работи чрез индукция по k.

Задача 269. Нека $\omega(n)$ е функцията от определение 24. Да се докаже, че при всяко $x \in \mathbb{R}$, $x \geq 10$ е в сила асимптотичнта формула

$$\sum_{n\leq x} \omega(n) = x \ln\ln x + cx + \mathcal{O}\Big(\frac{x}{\ln x}\Big)\,,$$

където c е константата от задача 248.

Решение: Като използуваме задачи 77, 248 и теоремата на Чебишев, получаваме

$$\begin{aligned}\sum_{n\leq x} \omega(n) &= \sum_{n\leq x}\sum_{p\mid n} 1 = \sum_{p\leq x} \sum_{\substack{n\leq x \\ n\equiv 0 \pmod p}} 1 \;= \\ &= \sum_{p\leq x} \Big[\frac{x}{p}\Big] = \sum_{p\leq x} \Big(\frac{x}{p} - \Big\{\frac{x}{p}\Big\}\Big) = x \sum_{p\leq x} \frac{1}{p} + \mathcal{O}(\pi(x)) \;= \\ &= x \ln\ln x + cx + \mathcal{O}\Big(\frac{x}{\ln x}\Big)\,.\end{aligned}$$

Определение 45. Казваме, че числото $n \in \mathbb{N}$ е *свободно от k–ти степени*, ако всеки прост множител на n влиза в каноничното му развитие в степен, която не надминава k. Нека $x \in \mathbb{R}$, $x \geq 1$. Означаваме с $N(x;k)$ броя на числата $n \in \mathbb{N}$, които са свободни от k–ти степени и за които $n \leq x$.

Забележка: В последното определение се обобщава понятието безквадратно число от определение 14.

Задача 270. Да се докаже, че при $k \in \mathbb{N}$, $k \geq 2$ е в сила асимптотичната формула

$$N(x;k) = c_k x + \mathcal{O}\big(x^{\frac{1}{k}}\big)\,,$$

където $c_k = \zeta(k)^{-1}$.

Упътване: Като използуваме определение 25 и задача 77, получаваме

$$N(x;k) = \sum_{n\leq x}\sum_{d^k|n}\mu(d) = \sum_{d\leq \sqrt[k]{x}}\mu(d)\sum_{\substack{n\leq x\\ n\equiv 0 \pmod{d^k}}} 1 = \sum_{d\leq \sqrt[k]{x}}\mu(d)\left[\frac{x}{d^k}\right],$$

след което работим както при решенията на предходните задачи.

Забележка: За някои числови функции е много трудно да се намерят асимптотични формули или оценки, подобни на разгледаните в настоящия параграф. Да разгледаме, например, сумата

$$M(x) = \sum_{n\leq x}\mu(n).$$

Очевидно, при $x \in \mathbb{R}$, $x \geq 1$ имаме $|M(x)| \leq x$. Известно е, че намирането на нетривиална оценка за $M(x)$ е в пряка връзка с оценяването на остатъчния член в асимптотичната формула за $\pi(x)$. В частност, може да се докаже, че $\lim_{x\to\infty}\frac{M(x)}{x} = 0$ и от това равенство по елементарен начин се установява асимптотичния закон за разпределение на простите числа. Да отбележим също, че хипотезата на Риман е еквивалентна на оценката $M(x) = \mathcal{O}\left(x^{\frac{1}{2}+\varepsilon}\right)$, където $\varepsilon > 0$ е произволно малко.

Литература

[1] К. Айерленд, М. Роузен, *Класическое введение в современную теорию чисел*, „Мир“, Москва, 1987.

[2] З.И. Боревич, И.Р. Шафаревич, *Теория чисел*, „Наука“, Москва, 1985.

[3] И.М. Виноградов, *Основы теории чисел*, „Наука“, Москва, 1981.

[4] М. Гаврилов, Л. Давидов, *Делимост на числата*, „Народна Просвета“, София, 1976.

[5] М. Гаврилов, Д. Димитров, И. Димовски, *Съвременна аритметика*, „Народна Просвета“, София, 1975.

[6] А.И. Галочкин, Ю.В Нестеренко, А.Б. Шидловский, *Введение в теорию чисел*, „Изд. Московского университета“, Москва, 1984.

[7] Г. Генов, С. Миховски, Т. Моллов, *Алгебра и теория на числата*, „Наука и изкуство“, София, 1991.

[8] С. Додунеков, К. Чакърян, *Задачи по теория на числата*, „Регалия 6“, София, 1999.

[9] *Избранные задачи из журнала "American Mathematical Monthly"* „Мир“, Москва, 1977.

[10] А.А. Карацуба, *Основы аналитической теории чисел*, „Наука“, Москва, 1983.

[11] Н. Коблиц, *p–адические числа, p–адический анализ и дзета–функции*, „Мир“, Москва, 1981.

[12] Т. Нагел, *Увод в теорията на числата*, „Наука и изкуство“, София, 1971.

[13] Н. Начев, *Теория на числата*, Ун. изд. ПУ „П. Хилендарски“, Пловдив, 2002.

[14] Д. Пойа, Г. Сегьо, *Задачи и теореми по анализ I*, „Наука и изкуство“, София, 1973.

[15] Д. Пойа, Г. Сегьо, *Задачи и теореми по анализ II*, „Наука и изкуство“, София, 1974.

[16] А.Г. Постников, *Введение в аналитическую теорию чисел*, „Наука“, Москва, 1971.

[17] К. Прахар, *Распределение простых чисел*, „Мир“, Москва, 1967.

[18] Н. Обрешков, *Теория на числата*, „Наука и изкуство“, София, 1996.

[19] Н. Обрешков, *Задачи и теореми по висша алгебра*, „Наука и изкуство“, София, 1966.

[20] В.А. Садовничий, А.С. Подкользин, *Задачи студенческих олимпиад по математике*, „Наука“, Москва, 1978.

[21] Э. Трост, *Простые числа*, Москва, 1959.

[22] К. Чандрасекхаран, *Введение в аналитическую теорию чисел*, „Мир“, Москва, 1974.

[23] Д.О. Шклярский, Н.Н. Ченцов, И.М. Яглом, *Избранные задачи и теоремы элементарной математики*, „Наука“, Москва, 1976.

[24] T. M. Apostol, *Introduction to analytic number theory*, Springer, 1976.

[25] M. Aigner, G, Ziegler, *Proofs from the Book*, Sec. ed., Springer, 2000.

[26] G. H. Hardy, E. M. Wright, *An introduction to the theory of numbers*, Fifth. ed., Oxford Univ. Press, 1979.

[27] G. Tenenbaum, *Introduction to Analytic and Probabilistic Number Theory*, Cambridge University Press, 1995.