

В. А. Ясінський, В. М. Лейфура,
І. М. Мітельман, О. Б. Панасенко, В. М. Радченко

**СЕКРЕТИ ПІДГОТОВКИ
ШКОЛЯРІВ ДО ВСЕУКРАЇНСЬКИХ
ТА МІЖНАРОДНИХ
МАТЕМАТИЧНИХ ОЛІМПІАД**

ТЕОРІЯ ЧИСЕЛ

Навчально-методичний посібник

Вінниця
ТОВ «Нілан-ЛТД»
2018

УДК 372.851:511(07)

C28

Рекомендовано до видання

Вченою радою Одеського обласного інституту удосконалення вчителів
(протокол від 22 червня 2017 р. №3)

та

Вченою радою Вінницького державного педагогічного університету
імені Михайла Коцюбинського
(протокол від 22 листопада 2017 р. №5)

Рецензенти:

Працьовитий М. В., заслужений діяч науки і техніки України, професор Національного педагогічного університету імені М. П. Драгоманова, доктор фізико-математичних наук;

Матяш О. І., професор Вінницького державного педагогічного університету імені Михайла Коцюбинського, доктор педагогічних наук;

Задоріна О. М., доцент Одеського обласного інституту удосконалення учителів, кандидат педагогічних наук.

C28 Секрети підготовки школярів до Всеукраїнських та Міжнародних математичних олімпіад. Теорія чисел : навч.-метод. посібник / В. А. Ясінський [та ін.] — Вінниця : ТОВ «Нілан-ЛТД», 2018. — 336 с.

ISBN 978-966-924-693-6

У посібнику подаються вибрані методи розв'язування задач олімпіадного характеру з теорії чисел, викладено відповідний теоретичний матеріал, наводяться задачі з докладними розв'язаннями й задачі для самостійної роботи. Посібник стане в пригоді вчителям математики, учням загальноосвітніх шкіл, керівникам математичних гуртків, організаторам олімпіад, студентам математичних та педагогічних спеціальностей тощо.

УДК 372.851:511(07)

Зміст

Передмова	6
Основні позначення	8
Розділ 1. Цілочисельні послідовності і функції	9
1.1. Арифметичні функції в теорії чисел	9
1.1.1. Мультиплікативні функції та їхні властивості	9
1.1.2. Кількість дільників $\tau(n)$ натурального числа	11
1.1.3. Сума дільників $\sigma(n)$ натурального числа	12
1.1.4. Добуток дільників $\pi(n)$ натурального числа	12
1.1.5. Функція Ейлера $\varphi(n)$	13
Задачі математичних олімпіад	17
1.2. Функція цілої частини дійсного числа в теорії чисел	25
Задачі математичних олімпіад	34
Задачі для самостійного розв'язування	43
Розділ 2. Арифметика цілих чисел	44
2.1. Подільність цілих чисел	44
2.1.1. Властивості відношення подільності цілих чисел	44
2.1.2. Ділення з остачею двох цілих чисел	46
Задачі математичних олімпіад	47
2.2. Прості і складені числа. Єдиність розкладу натурального числа на прості множники	54
Задачі математичних олімпіад	57
2.3. Найбільший спільний дільник і найменше спільне кратне натуральних чисел	72
2.3.1. Найбільший спільний дільник	72
2.3.2. Найменше спільне кратне	73
2.3.3. Алгоритм Евкліда знаходження найбільшого спільного дільника двох чисел	75
Задачі математичних олімпіад	78
2.4. Модулярна арифметика та її застосування до розв'язування олімпіадних задач	88

2.4.1. Конгруенції та їхні властивості	88
2.4.2. Повна і зведена системи лишків	90
2.4.3. Конгруенції з одним невідомим	92
Задачі математичних олімпіад	96
2.5. Степені цілих чисел	115
2.5.1. Точні квадрати	115
2.5.2. Точні куби	116
Задачі математичних олімпіад	117
2.6. Ознаки подільності натуральних чисел та інші системи числення	129
2.6.1. Системи числення	129
2.6.2. Ознаки подільності чисел в десятковій системі числення	131
2.6.3. Сума цифр натуральних чисел	134
Задачі математичних олімпіад	135
2.7. Показник числа за модулем, мала теорема Ферма, теорема Ейлера	145
2.7.1. Показник числа за модулем	145
2.7.2. Мала теорема Ферма	147
2.7.3. Теорема Ейлера	149
Задачі математичних олімпіад	151
2.8. Теорема Вільсона	179
Задачі математичних олімпіад	181
2.9. Китайська теорема про остачі	198
Задачі математичних олімпіад	200
2.10. Квадратичні лишки і нелишки та символ Лежандра	208
Задачі математичних олімпіад	211
2.11. Спеціальні числа в теорії чисел	218
2.11.1. Числа Ферма	218
2.11.2. Числа Мерсенна	221
2.11.3. Досконалі числа	226
2.12. Леми про показник степеня простого дільника	239
Задачі математичних олімпіад	244
Задачі для самостійного розв'язування	255

Розділ 3. Діофантові рівняння та методи їх розв'язування 259

3.1. Лінійні діофантові рівняння	259
Задачі математичних олімпіад	262
3.2. Рівняння Піфагора	268
Задачі математичних олімпіад	270

3.3. Деякі види квадратних діофантових рівнянь і задачі, що пов'язані з ними	275
Задачі математичних олімпіад	280
3.4. Рівняння Пелля	286
3.4.1. Рівняння виду: $x^2 - 2y^2 = 1$	287
3.4.2. Рівняння виду $x^2 - Dy^2 = 1$	289
Задачі математичних олімпіад	295
3.5. Метод оцінок і взаємно простих множників	298
Задачі математичних олімпіад	301
3.6. Принцип нескінченного спуску Ферма	324
Задачі математичних олімпіад	325
Задачі для самостійного розв'язування	332
Література	334
Показчик	335

Передмова

У 2011 р. побачив світ навчально-методичний посібник В. А. Ясінського «Олімпіадні задачі з теорії чисел. Практикум із розв'язування». Автор присвятив його *Валентину Миколайовичу Лейфури* (1947–2011) — відомому українському вченому та педагогу, одному із засновників математичного олімпіадного й турнірного руху незалежної України.

У 2014–2015 рр. були видані ще дві книжки В'ячеслава Ясінського (у співавторстві із О. Б. Панасенком), об'єднані назвою «Секрети підготовки школярів до Всеукраїнських та Міжнародних математичних олімпіад» — з геометрії та алгебри. В'ячеслав Андрійович омріявав ще декілька книжок цієї ж самої серії, зокрема — працював над матеріалами теоретико-числової тематики, якими мав бути значно розширений зміст згаданого вище посібника з теорії чисел. На жаль, раптова смерть В'ячеслава Андрійовича Ясінського в листопаді 2015 р. завадила своєчасному здійсненню цих планів.

У пам'ять про В'ячеслава Андрійовича Ясінського — неперевершеного українського педагога-математика, заслуженого вчителя України, видатного композитора олімпіадних задач — завершити розпочату роботу було справою честі для його колег і друзів, однодумців, з якими він співпрацював.

Протягом багатьох років нам пощастило разом із В. А. Ясінським та В. М. Лейфурую брати участь в організації та проведенні олімпіад і турнірів, створювати нові задачі, готувати збірні команди України до Міжнародних математичних олімпіад. Як добре відомо, підготовка обдарованих учнів саме з теорії чисел є одним з наріжних каменів, запорукою успіхів на таких авторитетних змаганнях. Тому опрацюванню складних розділів елементарної теорії чисел, методики та практики розв'язування олімпіадних теоретико-числових задач найвищого рівня складності завжди приділялося нами чимало уваги: читалися цікаві ґрунтовні лекції, пропонувалися задачні «ланцюжки», спільно вивчалися й узагальнювалися задачі математичних олімпіад різних країн, робочі матеріали Міжнародних олімпіад тощо. Такі розробки знайшли своє місце в цьому посібнику, у багатьох випадках — з оновленням відповідних задачних матеріалів, що краще відтворює актуальні сучасні тенденції щодо змісту математичних змагань високого рівня. Важко переоцінити вагомий внесок професора В. М. Лейфури — наукового керівника збірної команди України

на Міжнародних олімпіадах 2003–2006 рр. — до створення та багаторічного наукового супроводу вітчизняної системи підготовки юних математиків нашої країни до участі в Міжнародних математичних олімпіадах. Його глибокі математичні й методичні ідеї завжди надихали на плідну творчу роботу.

Запропонований навчально-методичний посібник стане в пригоді вчителям математики, керівникам математичних гуртків, методичним працівникам, організаторам олімпіад і турнірів з математики, учням, які готуються до математичних змагань, студентам математичних та педагогічних спеціальностей університетів, усім тим, хто цікавиться розв'язуванням складних задач з математики.

Ігор Мітельман
Олексій Панасенко
Вадим Радченко

Основні позначення

\mathbb{N}	множина всіх натуральних чисел
\mathbb{Z}	множина всіх цілих чисел
\mathbb{Z}_+	множина всіх цілих невід'ємних чисел
\mathbb{Q}	множина всіх раціональних чисел
\mathbb{R}	множина всіх дійсних чисел
$\tau(n)$	кількість усіх натуральних дільників числа n
$\sigma(n)$	сума всіх натуральних дільників числа n
$\varphi(n)$	кількість усіх натуральних чисел, які менші за n і взаємно прості з n
$[x]$	ціла частина числа x , тобто найбільше ціле число, що не перевищує x
$\{x\}$	дробова частина числа x , $\{x\} = x - [x]$
$n!$	добуток $1 \cdot 2 \cdot \dots \cdot n$, $n > 1$; $1! = 1$, $0! = 1$
$\sum_{k=1}^n a_k$	$a_1 + a_2 + \dots + a_n$
$\prod_{k=1}^n a_k$	$a_1 \cdot a_2 \cdot \dots \cdot a_n$
$a : b$	ціле число a ділиться без остачі на ціле число $b \neq 0$
$b \mid a$	число b ділить число a (b є дільником числа a)
НСД(a, b) або (a, b)	найбільший спільний дільник чисел a, b
НСК(a, b) або $[a, b]$	найменше спільне кратне чисел a, b
$a \equiv b \pmod{m}$	цілі числа a і b конгруентні за модулем m , $m > 1$
(a_n) або $\{a_n\}$	числова послідовність $a_1, a_2, \dots, a_n, \dots$
$\min\{a_1, \dots, a_n\}$	найменше з чисел a_1, \dots, a_n
$\max\{a_1, \dots, a_n\}$	найбільше з чисел a_1, \dots, a_n
$\left(\frac{a}{p}\right)$	символ Лежандра

ЦІЛОЧИСЕЛЬНІ ПОСЛІДОВНОСТІ І ФУНКЦІЇ

1.1. Арифметичні функції в теорії чисел

Будь-яка функція $f : \mathbb{N} \rightarrow \mathbb{R}$ називається *арифметичною*.

Вивчаючи властивості цілих чисел, доводиться розглядати різні арифметичні функції. Прикладами таких функцій є кількість $\tau(n)$ додатних дільників натурального числа n , сума $\sigma(n)$ додатних дільників натурального числа n , добуток $\pi(n)$ додатних дільників натурального числа n , число $\varphi(n)$ додатних дільників натурального числа n , які взаємно прості з n , тощо.

1.1.1. Мультиплікативні функції та їхні властивості

Арифметична функція f називається *мультиплікативною*, якщо вона задовольняє наступним двом умовам:

1. Значення функції не дорівнює нулю щонайменше при одному $n > 1$.
2. Для довільних додатних взаємно простих a та b , маємо:

$$f(ab) = f(a)f(b).$$

Легко бачити, що функція $f(n) = n^s$, де s — довільне дійсне число, є мультиплікативною.

Теорема 1.1. Якщо $f(n)$ є мультиплікативною функцією, то $f(1) = 1$.

Доведення. Справді, за означенням існує таке n_0 , для якого $f(n_0) \neq 0$. Тоді $f(n_0) = f(n_0 \cdot 1) = f(n_0)f(1)$, звідки, після скорочення, знаходимо: $f(1) = 1$. \square

Умова 2 із означення мультиплікативної функції $f(n)$ має місце і при $k > 2$ попарно взаємно простих чисел $n_1, n_2, n_3, \dots, n_k$. Справді,

$$\begin{aligned} f(n_1 n_2 n_3 \dots n_k) &= f(n_1) f(n_2 n_3 \dots n_k) = f(n_1) f(n_2) f(n_3 \dots n_k) = \dots = \\ &= f(n_1) f(n_2) f(n_3) \dots f(n_k). \end{aligned}$$

Легко перевірити, що для різних простих чисел p_1, \dots, p_k :

$$f(p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \dots p_k^{\alpha_k}) = f(p_1^{\alpha_1}) f(p_2^{\alpha_2}) f(p_3^{\alpha_3}) \dots f(p_k^{\alpha_k}). \quad (1.1)$$

Навпаки, ми завжди можемо побудувати деяку мультиплікативну функцію $f(n)$, якщо покладемо $f(1) = 1$ і означимо довільно значення для $f(p^\alpha)$, що відповідають додатнім степеням простих чисел, в загальному випадку означивши її рівністю (1.1).

Наприклад, мультиплікативну функцію можна побудувати, взявши $f(1) = 1$ і $f(p^\alpha) = 2$, якщо $\alpha > 0$. Тоді для будь-якого натурального k будемо мати $f(p_1^{\alpha_1} \cdot \dots \cdot p_k^{\alpha_k}) = 2^k$. Зокрема знаходимо:

$$\begin{aligned} f(1) &= 1, & f(2) &= 2, & f(3) &= 2, & f(4) &= 2, \\ f(5) &= 2, & f(6) &= 4, & f(7) &= 2, & f(8) &= 2, \\ f(9) &= 2, & f(10) &= 4, & f(11) &= 2, & f(12) &= 4, \dots \end{aligned}$$

Теорема 1.2. Добуток $f_1(n)f_2(n)\dots f_k(n)$ мультиплікативних функцій $f_1(n), f_2(n), \dots, f_k(n)$ є мультиплікативною функцією.

Доведення. Розглянемо випадок коли $k = 2$. Покажемо, що добуток $f(n) = f_1(n)f_2(n)$ є мультиплікативною функцією. Дійсно, $f(1) = f_1(1)f_2(1) = 1$. Крім того, при взаємно простих n_1 і n_2 , одержимо:

$$\begin{aligned} f(n_1n_2) &= f_1(n_1n_2)f_2(n_1n_2) = f_1(n_1)f_1(n_2)f_2(n_1)f_2(n_2) = \\ &= f_1(n_1)f_2(n_1)f_1(n_2)f_2(n_2) = f(n_1)f(n_2). \end{aligned}$$

Для $k > 2$, використовуючи попереднє твердження, індуктивно знаходимо:

$$\begin{aligned} f_1(n)f_2(n)f_3(n) &= (f_1(n)f_2(n))f_3(n), \\ f_1(n)f_2(n)f_3(n)f_4(n) &= (f_1(n)f_2(n)f_3(n))f_4(n), \\ &\vdots \\ f_1(n)f_2(n)\dots f_{k-1}(n)f_k(n) &= (f_1(n)f_2(n)\dots f_{k-1}(n))f_k(n). \end{aligned}$$

□

Теорема 1.3. Нехай $f(n)$ — мультиплікативна функція і $p_1^{\alpha_1} \cdot \dots \cdot p_k^{\alpha_k}$ — канонічний розклад числа n . Тоді, позначивши символом $\sum_{d|a}$ суму, що поширюється на всі дільники d числа a , одержимо:

$$\begin{aligned} \sum_{d|n} f(d) &= (1 + f(p_1) + f(p_1^2) + \dots + f(p_1^{\alpha_1})) \cdot \dots \times \\ &\quad \times (1 + f(p_k) + f(p_k^2) + \dots + f(p_k^{\alpha_k})). \end{aligned}$$

(У випадку $n = 1$ права частина вважається рівною 1.)

Зауваження. Як бачимо, права частина цієї формули є добутком k множників у дужках. А тому цю формулу записують у вигляді:

$$\sum_{d|n} f(d) = \prod_{i=1}^k (1 + f(p_i) + f(p_i^2) + \dots + f(p_i^{\alpha_i})).$$

Доведення. Для доведення цього твердження, розкриємо дужки в її правій частині. Тоді одержимо суму всіх доданків виду

$$f(p_1^{\beta_1}) f(p_2^{\beta_2}) \dots f(p_k^{\beta_k}) = f(p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}),$$

де $0 \leq \beta_1 \leq \alpha_1, 0 \leq \beta_2 \leq \alpha_2, \dots, 0 \leq \beta_k \leq \alpha_k$. А це і будуть всі дільники числа n , тобто рівність виконується. \square

1.1.2. Кількість дільників $\tau(n)$ натурального числа.

Розглянемо мультиплікативну функцію $f(n) = 1$, де $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ — канонічний розклад числа n . Тоді формула теореми 1.3 буде мати вигляд:

$$\begin{aligned} \sum_{d|n} f(d) &= \prod_{i=1}^k (1 + f(p_i) + f(p_i^2) + \dots + f(p_i^{\alpha_i})) = \\ &= \prod_{i=1}^k \left(1 + \underbrace{1 + 1 + \dots + 1}_{\alpha_i} \right) = (\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_k + 1) = \tau(n). \end{aligned}$$

Отже, $\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_k + 1)$ — це кількість дільників натурального числа n .

Зрозуміло, що $\tau(n)$ є непарним числом тоді і тільки тоді, коли n є точним квадратом, бо усі $\alpha_1 + 1, \dots, \alpha_k + 1$ — непарні, а тому усі $\alpha_1, \dots, \alpha_k$ — парні.

Очевидно, що $\tau(n) \leq n$, причому рівність досягається лише при $n = 1$ і $n = 2$.

Теорема 1.4. $\tau(n)$ — мультиплікативна функція.

Доведення. Умова 1 означення мультиплікативної функції $\tau(1) = 1$ є очевидною. Розглянемо доведення умови 2. Дійсно, розглянемо два взаємно простих числа m і n , а a_1, a_2, \dots, a_k — всі дільники числа m і b_1, b_2, \dots, b_l — всі дільники числа n . Тоді довільний дільник числа mn є $a_i b_j$, $1 \leq i \leq k$, $1 \leq j \leq l$, тобто $\tau(m) = k$, $\tau(n) = l$, $\tau(mn) = kl$, тобто $\tau(mn) = \tau(m) \tau(n)$.

Доведемо, що $\tau(n)$ — мультиплікативна функція, іншим способом, використовуючи формулу (1.1).

Справді, нехай $m = p_1^{\alpha_1} \cdot \dots \cdot p_k^{\alpha_k}$ і $n = q_1^{\beta_1} \cdot \dots \cdot q_s^{\beta_s}$ — два взаємно простих числа, тоді числа $p_1, \dots, p_k, q_1, \dots, q_s$ є різними. Тоді канонічний розклад числа

$$mn = p_1^{\alpha_1} \cdot \dots \cdot p_k^{\alpha_k} q_1^{\beta_1} \cdot \dots \cdot q_s^{\beta_s}.$$

Звідси слідує, що

$$\tau(mn) = (\alpha_1 + 1) \dots (\alpha_k + 1) (\beta_1 + 1) \dots (\beta_s + 1) = \tau(m) \tau(n).$$

□

Із знайденої для $\tau(n)$ формули безпосередньо слідує, що при простому p і натуральному α : $\tau(p^\alpha) = \alpha + 1$.

1.1.3. Сума дільників $\sigma(n)$ натурального числа.

Функцію $\sigma(n)$ означимо як суму усіх натуральних дільників числа n .

Теорема 1.5. Функція $\sigma(n)$ є мультиплікативною, і якщо $p_1^{\alpha_1} \cdot \dots \cdot p_k^{\alpha_k}$ — канонічний розклад числа n , то

$$\sigma(n) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \dots \cdot \frac{p_k^{\alpha_k+1} - 1}{p_k - 1}.$$

Доведення. Умова 1 означення мультиплікативної функції $\sigma(1) = 1$ є очевидною. Розглянемо доведення умови 2. Дійсно, розглянемо два взаємно простих числа m і n , а a_1, a_2, \dots, a_k — всі дільники числа m і b_1, b_2, \dots, b_l — всі дільники числа n . Тому довільний дільник числа mn буде мати вигляд $a_i b_j$, $1 \leq i \leq k$, $1 \leq j \leq l$, тобто, що і треба було довести.

Функція $f(n) = n$ задовольняє умовам мультиплікативної функції. Тому розглянемо для неї формулу теореми 1.3. Для $n = p_1^{\alpha_1} \cdot \dots \cdot p_k^{\alpha_k}$, одержуємо:

$$\sigma(n) = \sum_{d|n} d = \prod_{i=1}^k (1 + p_i + p_i^2 + \dots + p_i^{\alpha_i}) = \prod_{i=1}^k \frac{p_i^{\alpha_i+1} - 1}{p_i - 1},$$

що і треба було довести. □

Натуральне число a називається *досконалим*, якщо $\sigma(a) = 2a$. Деякі властивості досконалих чисел детальніше розглядатимуться в п. 2.11.3.

1.1.4. Добуток дільників $\pi(n)$ натурального числа.

Через $\pi(n)$ позначимо добуток усіх натуральних дільників натурального числа n . Передусім зазначимо, що функція $\pi(n)$ не є мультиплікативною функцією, оскільки, наприклад, $\pi(2) \pi(3) = 6 \neq \pi(2 \cdot 3) = 36$.

Теорема 1.6. Для функції $\pi(n)$ має місце наступна формула:

$$\pi(n) = n^{\frac{1}{2}\tau(n)}.$$

Доведення. Справді, якщо d_1, d_2, \dots, d_s — всі різні дільники числа n , то $s = \tau(n)$ і $d_1 d_2 \dots d_s = \frac{n}{d_1} \frac{n}{d_2} \dots \frac{n}{d_s}$, звідки $\pi(n)^2 = n^{\tau(n)}$. \square

Теорема 1.7. Функція $\pi(n)$ є ін'єктивною, тобто якщо $\pi(m) = \pi(n)$, то $m = n$.

Доведення. Оскільки $\pi(m) = \pi(n)$, то $n^{\tau(n)/2} = m^{\tau(m)/2}$, тобто $n^{\tau(n)} = m^{\tau(m)}$. Звідси випливає, що m і n мають однакові прості дільники. Нехай деяке просте число p входить до розкладу числа n з показником α , а до m з показником β , тоді $\alpha \cdot \tau(n) = \beta \cdot \tau(m)$, тобто дріб $\frac{\alpha}{\beta} = \frac{\tau(m)}{\tau(n)}$ не залежить від α і β . Якщо припустити, що цей дріб відмінний від 1, то одержимо протиріччя. Тому $\alpha = \beta$ для всіх простих дільників p , тобто $m = n$. \square

Наприклад, знайдемо усі такі n , що $\pi(n) = 5832$. Оскільки $5832 = 18^3$, то $n^{\tau(n)} = 18^6$. Помічаючи, що $\tau(18) = 6$, і використовуючи ін'єктивність функції $\pi(n)$, знаходимо, що єдине таке число n — 18.

1.1.5. Функція Ейлера $\varphi(n)$.

Функція Ейлера $\varphi(n)$ визначена для всіх натуральних n і представляє собою кількість чисел ряду $1, 2, \dots, n-1$, взаємно простих з n . Наприклад:

$$\begin{aligned}\varphi(1) &= 1, & \varphi(2) &= 1, & \varphi(3) &= 2, \\ \varphi(4) &= 2, & \varphi(5) &= 4, & \varphi(6) &= 2.\end{aligned}$$

Теорема 1.8. Нехай p — просте число, k — натуральне. Тоді

$$\varphi(p^k) = p^k - p^{k-1}.$$

Доведення. Зрозуміло, що взаємно прості числа з числом p^k , це числа, які не діляться на p . Числа, які кратні p і менші p^k , це числа: $p, 2p, \dots, (p-1)p, p^2, \dots, p^{k-1}$. Їх кількість дорівнює $\left[\frac{p^k}{p}\right] - 1 = p^{k-1} - 1$. А тому кількість чисел, які менші p^k і не діляться на p , буде дорівнювати

$$\varphi(p^k) = (p^k - 1) - (p^{k-1} - 1) = p^k - p^{k-1},$$

що і завершує доведення. \square

Обчислювати значення функції Ейлера для натуральних чисел іншого виду просто в силу її мультиплікативності.

Теорема 1.9. Функція φ мультиплікативна, тобто для будь-яких натуральних взаємно простих чисел a і b має місце рівність

$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b).$$

Доведення. Перший спосіб. Розглянемо числа $T(x, y) = ax + by$, де a і b — взаємно прості, $x = 1, 2, \dots, b - 1$, $y = 1, 2, \dots, a - 1$, a . Всі такі числа дають різні остачі від їх ділення на ab . Дійсно, якщо існують такі x_1, y_1 та x_2, y_2 із своїх наборів, що $ax_1 + by_1 \equiv ax_2 + by_2 \pmod{ab}$, тоді за цим модулем $a(x_1 - x_2) + b(y_1 - y_2) \equiv 0$, тобто $(a(x_1 - x_2) + b(y_1 - y_2)) : ab$. Перший доданок ділиться на a , тоді і другий доданок ділитиметься на a . А в силу взаємної простоти чисел a і b , одержуємо, що $(y_1 - y_2) : a$, що можливо лише при $y_1 = y_2$, бо $y_1, y_2 \in \{1, 2, \dots, a - 1, a\}$. Тоді $(x_1 - x_2) : b$, що також можливо лише при $x_1 = x_2$, бо $x_1, x_2 \in \{1, 2, \dots, b - 1, b\}$.

Далі, доведемо, що $T(x, y)$ взаємно просте з ab тоді і тільки тоді, коли x взаємно просте з b , а y взаємно просте з a . Дійсно, нехай $T(x, y)$ взаємно просте з ab , але (не порушуючи загальності) x і b мають спільний дільник $d > 1$. Але тоді $T(x, y) : d$, що суперечить припущенню, бо $ab : d$. Навпаки, нехай x взаємно просте з b і y взаємно просте з a , але $T(x, y)$ і ab мають спільний дільник $d > 1$. Нехай p — довільний простий дільник числа $d > 1$, тоді $p \mid ab$. Не порушуючи загальності, будемо вважати, що $p \mid a$, тоді p не ділить y (в силу їхньої взаємної простоти). Тому з того, що $p \mid (ax + by)$ випливає, що $p \mid by$. Звідси слідує, що $p \mid b$, а це суперечить тому, що числа a і b є взаємно простими.

Таким чином, кількість різних остач при діленні $T(x, y)$ на ab буде рівною $\varphi(ab)$, чисел x , взаємно простих b , буде рівно $\varphi(b)$, чисел y , взаємно простих з a , буде рівно $\varphi(a)$. Тому, $\varphi(ab) = \varphi(a) \cdot \varphi(b)$, бо для кожного x (а їх $\varphi(b)$) буде $\varphi(a)$ чисел y .

Другий спосіб. Розташуємо усі натуральні числа від 1 до $a \cdot b$ в такий спосіб: в 1-му рядку від 1 до b , в 2-му — від $b + 1$ до $2 \cdot b$, ..., в a -му — від $(a - 1) \cdot b$ до $a \cdot b$. Тоді в кожному рядку $\varphi(b)$ чисел, взаємно простих з b , а в кожному стовпчику $\varphi(a)$ чисел, взаємно простих a (справді, числа у кожному стовпчику дають попарно різні остачі при діленні на a). Оскільки a і b взаємно прості, то число буде взаємно просте з $a \cdot b$ тоді і тільки тоді, коли воно стоїть на перетині стовпчика з номером, який взаємно простий з b , і рядка з номером, який взаємно простий з a . Оскільки в цій таблиці $\varphi(a \cdot b)$ чисел взаємно простих з $a \cdot b$, то за правилом добутку їх буде $\varphi(a) \cdot \varphi(b)$. Отже, $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$, де a і b взаємно прості. \square