

ДРУШТВО МАТЕМАТИЧАРА СРБИЈЕ  
Материјали за младе математичаре, свеска 15

---

Владимир Мићић                      Зоран Каделбург  
Душан Ђукић

# УВОД У ТЕОРИЈУ БРОЈЕВА

Пето, допуњено издање

Б Е О Г Р А Д  
2013.

*др Владимир Мићић*, професор Грађевинског факултета у Београду  
*др Зоран Каделбург*, професор Математичког факултета у Београду  
*Душан Ђукић*, асистент Машинског факултета у Београду

## УВОД У ТЕОРИЈУ БРОЈЕВА

пето, допуњено издање

Материјали за младе математичаре, свеска 15

Издавач: ДРУШТВО МАТЕМАТИЧАРА СРБИЈЕ

Београд, Кнеза Михаила 35/IV

<http://www.dms.org.rs>

За издавача: *др Александар Липковски*

Рецензент: *др Љубомир Чукић*

Уредник: *др Зоран Каделбург*

AMS-класификација: 11–01

УДК: 511.2

© Друштво математичара Србије

Ранија издања: 1983, 1989, 2001, 2004.

ISBN 978–86–81453–89–6

CIP – Каталогизација у публикацији

Народна библиотека Србије, Београд



Штампање ове књиге помогла је  
Нафтна индустрија Србије

511.2/.5

МИЋИЋ, Владимир, 1936–

Увод у теорију бројева / Владимир Мићић,  
Зоран Каделбург, Душан Ђукић. – 5. допуњено  
изд. – Београд : Друштво математичара Србије,  
2013. (Нови Сад : Стојков). – VI, 207 стр. : 25 см.  
– (Материјали за младе математичаре / Друштво  
математичара Србије ; св. 15)

Тираж 1000. – Напомене уз текст. –

Библиографија: стр. 205–207. – Регистри.

ISBN 978–86–81453–89–6

1. Каделбург, Зоран [аутор], 1950–

2. Ђукић, Душан [аутор], 1981–

а) Теорија бројева

COBISS.SR-ID 196493580

Тираж: 1000 примерака

Штампа: „Стојков“, Нови Сад

## С А Д Р Ж А Ј

ПРЕДГОВОР . . . . .	v
1. ДЕЉИВОСТ ЦЕЛИХ БРОЈЕВА . . . . .	1
Задачи . . . . .	7
2. ПРОСТИ БРОЈЕВИ . . . . .	11
Задачи . . . . .	19
3. КОНГРУЕНЦИЈЕ . . . . .	25
Релација конгруенције . . . . .	25
Остаци квадрата . . . . .	26
Системи остатака. Ојлерова и Фермаова теорема . . . . .	28
Поредак броја по датом модулу . . . . .	31
Кармајклова теорема . . . . .	34
Вилсонова теорема . . . . .	35
Критеријуми дељивости . . . . .	36
Укратко о применама у криптографији . . . . .	38
Конгруенције вишег степена по модулу $p^k$ . . . . .	38
Егзистенција примитивног корена по простом модулу . . . . .	40
Задачи . . . . .	42
4. ДИОФАНТОВЕ ЈЕДНАЧИНЕ . . . . .	49
Линеарне Диофантове једначине . . . . .	49
Систем линеарних конгруенција . . . . .	52
Питагорине тројке . . . . .	54
Опште квадратне Диофантове једначине . . . . .	55
Велика Фермаова теорема . . . . .	57
Метода минималног решења . . . . .	58
Даље о целобројним решењима једначина . . . . .	60
Задачи . . . . .	61
5. КВАДРАТНЕ КОНГРУЕНЦИЈЕ . . . . .	67
Квадратне конгруенције по простом модулу . . . . .	67
Квадратне конгруенције по сложеном модулу . . . . .	73
Неке суме Лежандрових симбола . . . . .	75
Лагранжова теорема . . . . .	78
Задачи . . . . .	80

6. ДИОФАНТОВЕ АПРОКСИМАЦИЈЕ . . . . .	83
Рационални и ирационални бројеви . . . . .	83
Фарејев низ . . . . .	89
Алгебарски и трансцендентни бројеви . . . . .	93
Пелова једначина . . . . .	97
Једначине Пеловог типа . . . . .	102
Трансцендентност броја $e$ и ирационалност броја $\pi$ . . . . .	106
Задачи . . . . .	108
7. КВАДРАТНА РАШИРЕЊА ПОЉА РАЦИОНАЛНИХ БРОЈЕВА . . . . .	111
Цели елементи у $\mathbf{Q}[\sqrt{d}]$ . . . . .	112
Поредак и норма . . . . .	114
Деливост . . . . .	115
Јединственост растављања на просте чиниоце . . . . .	117
Последице основне теореме аритметике . . . . .	119
Велика Фермаова теорема за $n = 3$ . . . . .	120
Конгруенције вишег степена . . . . .	122
Примена на линеарне рекурентне низове другог реда . . . . .	124
Укратко о општим алгебарским раширењима . . . . .	125
Задачи . . . . .	126
8. ЗАДАЦИ СА МЕЂУНАРОДНИХ И БАЛКАНСКИХ МАТЕМАТИЧКИХ ОЛИМПИЈАДА . . . . .	129
Међународне олимпијаде . . . . .	129
Балканске олимпијаде . . . . .	136
Јуниорске балканске олимпијаде . . . . .	139
9. РЕЗУЛТАТИ И УПУТСТВА ЗА РЕШАВАЊЕ ЗАДАТАКА . . . . .	143
1. глава . . . . .	143
2. глава . . . . .	146
3. глава . . . . .	153
4. глава . . . . .	163
5. глава . . . . .	170
6. глава . . . . .	174
7. глава . . . . .	178
8. глава . . . . .	182
ИНДЕКС ПОЈМОВА . . . . .	201
ИНДЕКС ИМЕНА . . . . .	203
ЛИТЕРАТУРА . . . . .	205

## ИЗ ПРЕДГОВОРА ПРВОМ ИЗДАЊУ

Теорија бројева је, уз геометрију, свакако најстарија математичка дисциплина. Њене темеље поставили су још старогрчки математичари – Питагора, Еуклид, Диофант и други. Но, упркос томе, никако се не може рећи да је то данас завршена дисциплина. Постоје чак проблеми у њој који су постављени пре више од две хиљаде година, а који још увек нису решени. И баш то обиље проблема, и то проблема који се врло често могу формулисати тако да их разуме и математичар-почетник, давало је кроз историју сталан подстрек даљем развоју теорије бројева и чинило је интересантном све новим и новим генерацијама математичара.

Све наведено условило је да, откако су почела да се организују математичка такмичења, задаци из теорије бројева имају на њима доминантно место. Рекло би се чак да их последњих година има све више. Истовремено, моментално нема на нашем језику одговарајућег приручника који би омогућавао ученицима који се припремају за математичка такмичења и, уопште, свима онима који се нешто више занимају за математику, да се упознају са теоријским основама ове дисциплине. То је био главни разлог што смо се одлучили да напишемо ову књижицу.

Материјал у овој свесци писан је тако да углавном буде приступачан најмлађим ученицима средњих школа (па чак делом и основних). Но, претпостављамо да ће одређени делови бити занимљиви и старијим ученицима, па и онима који се припремају за више ступење такмичења, све до Међународне математичке олимпијаде. Наравно, ова свеска није ништа друго него оно што јој наслов каже – увод. За детаљније упознавање са теоријом бројева постоји веома велика литература, али, на жалост, углавном на страним језицима. Неке од књига за које мислимо да се непосредно настављају на овај материјал наведене су у списку литературе.

Ниједна књига из теорије бројева не би могла да се замисли без пратеће збирке задатака. У овој се налази око 130 задатака, изабраних тако да покривају теоријски материјал, али и добрим делом излазе ван њега. Такође су укључени неки задаци са наших такмичења (задаци са Републичких и Савезних такмичења су јасно означени), као и сви задаци са Међународних и Балканских математичких олимпијада који се тичу теорије бројева. На жалост, расположиви простор није омогућавао да се сви задаци дају са решењима, но скоро је сваки задатак снабдевен довољно детаљним упутством, а нумерички примери резултатом. Известан број тежих задатака је детаљно решен, а неки задаци су преузети из других свезака ове серије, па се решења тамо могу и наћи.

Београд, јуна 1983.

*Аутори*

**ПРЕДГОВОР ЧЕТВРТОМ ИЗДАЊУ**

Као и у ранијим издањима, књига је допуњена, како елементима теорије (овај пут у значајнијој мери), тако и новим задацима. У оквиру постојећих глава укључене су нове теме, као што су: Конгруенције по модулу  $p^k$ , Егзистенција примитивног корена по простом модулу, Опште квадратне Диофантове једначине, Метода минималног решења, Пелова једначина и Једначине Пеловог типа, а такође су додате две нове главе: Квадратне конгруенције и Раширења прстена целих бројева. Нови задаци илуструју овај допунски материјал, а додати су и многи задаци са разних домаћих и међународних такмичења, тако да задатака сада има око 400. Неки задаци из књига серије „Материјали за младе математичаре“ које су сада теже доступне снабдевени су упутствима за решавање. Такође, изванредан број задатака је пребачен у основни текст ради боље илустрације теоријског материјала.

Већи део теоријске допуне написао је Душан Ђукић који се у овом издању појављује као нови коаутор књиге.

Београд, октобра 2004.

*Аутори*

**ПРЕДГОВОР ПЕТОМ ИЗДАЊУ**

Ово издање је допуњено задацима са домаћих и међународних такмичења у протеклих неколико година. Прерађена је и допуњена глава 7 о раширењима поља.

Београд, јануара 2013.

*Аутори*