

# Sadržaj

<b>Predgovor</b>	<b>i</b>
<b>1 Uvod</b>	<b>1</b>
1.1 Peanovi aksiomi . . . . .	1
1.2 Princip matematičke indukcije . . . . .	4
1.3 Fibonaccijevi brojevi . . . . .	9
1.4 Zadatci . . . . .	17
<b>2 Djeljivost</b>	<b>21</b>
2.1 Najveći zajednički djeljitelj . . . . .	21
2.2 Euklidov algoritam . . . . .	24
2.3 Prosti brojevi . . . . .	29
2.4 Zadatci . . . . .	37
<b>3 Kongruencije</b>	<b>40</b>
3.1 Definicija i svojstva kongruencija . . . . .	40
3.2 Pravila za djeljivost . . . . .	43
3.3 Linearne kongruencije . . . . .	46
3.4 Kineski teorem o ostatcima . . . . .	48
3.5 Reducirani sustav ostataka . . . . .	51
3.6 Kongruencije po prostom modulu . . . . .	55
3.7 Primitivni korijeni i indeksi . . . . .	60
3.8 Decimalni zapis racionalnog broja . . . . .	65
3.9 Pseudoprosti brojevi . . . . .	69
3.10 Zadatci . . . . .	75
<b>4 Kvadratni ostatci</b>	<b>79</b>
4.1 Legendreov simbol . . . . .	79
4.2 Kvadratni zakon reciprociteta . . . . .	85
4.3 Računanje kvadratnog korijena modulo $p$ . . . . .	89

4.4	Jacobijev simbol . . . . .	91
4.5	Djeljivost Fibonaccijevih brojeva . . . . .	94
4.6	Zadatci . . . . .	99
<b>5</b>	<b>Kvadratne forme</b>	<b>102</b>
5.1	Sume dvaju kvadrata . . . . .	102
5.2	Pozitivno definitne kvadratne forme . . . . .	106
5.3	Sume četiriju kvadrata . . . . .	115
5.4	Sume triju kvadrata . . . . .	119
5.5	Zadatci . . . . .	127
<b>6</b>	<b>Aritmetičke funkcije</b>	<b>130</b>
6.1	Funkcija najveće cijelo . . . . .	130
6.2	Multiplikativne funkcije . . . . .	134
6.3	Asimptotske ocjene za aritmetičke funkcije . . . . .	139
6.4	Dirichletov produkt . . . . .	145
6.5	Zadatci . . . . .	148
<b>7</b>	<b>Distribucija prostih brojeva</b>	<b>152</b>
7.1	Elementarne ocjene za funkciju $\pi(x)$ . . . . .	152
7.2	Čebiševljeve funkcije . . . . .	157
7.3	Riemannova zeta-funkcija . . . . .	165
7.4	Dirichletovi karakteri . . . . .	169
7.5	Prosti brojevi u aritmetičkom nizu . . . . .	176
7.6	Zadatci . . . . .	180
<b>8</b>	<b>Diofantske aproksimacije</b>	<b>184</b>
8.1	Dirichletov teorem . . . . .	184
8.2	Fareyjevi nizovi . . . . .	187
8.3	Verižni razlomci . . . . .	194
8.4	Verižni razlomci i aproksimacija iracionalnih brojeva . . . . .	201
8.5	Ekvivalentni brojevi . . . . .	210
8.6	Periodski verižni razlomci . . . . .	215
8.7	Newtonovi aproksimanti . . . . .	221
8.8	Simultane aproksimacije . . . . .	225
8.9	LLL-algoritam . . . . .	232
8.10	Zadatci . . . . .	239
<b>9</b>	<b>Primjena diofantskih aproksimacija u kriptografiji</b>	<b>243</b>
9.1	Vrlo kratki uvod u kriptografiju . . . . .	243

9.2	Kriptosustav RSA . . . . .	247
9.3	Wienerov napad na kriptosustav RSA . . . . .	250
9.4	Napadi na RSA koji se koriste LLL-algoritmom . . . . .	253
9.5	Coppersmithov teorem . . . . .	256
9.6	Zadatci . . . . .	259
<b>10</b>	<b>Diofantske jednačbe I</b>	<b>263</b>
10.1	Linearne diofantske jednačbe . . . . .	263
10.2	Pitagorine trojke . . . . .	267
10.3	Pellova jednačba . . . . .	277
10.4	Verižni razlomci i Pellova jednačba . . . . .	285
10.5	Pelovska jednačba . . . . .	288
10.6	Kvadrati u Fibonaccijevu nizu . . . . .	294
10.7	Ternarne kvadratne forme . . . . .	298
10.8	Lokalno-globalni princip . . . . .	311
10.9	Zadatci . . . . .	319
<b>11</b>	<b>Polinomi</b>	<b>324</b>
11.1	Djeljivost polinoma . . . . .	324
11.2	Korijeni polinoma . . . . .	331
11.3	Ireducibilnost polinoma . . . . .	337
11.4	Dekompozicija polinoma . . . . .	340
11.5	Simetrični polinomi . . . . .	347
11.6	Zadatci . . . . .	352
<b>12</b>	<b>Algebarski brojevi</b>	<b>355</b>
12.1	Kvadratna polja . . . . .	355
12.2	Polja algebarskih brojeva . . . . .	365
12.3	Algebarski cijeli brojevi . . . . .	369
12.4	Ideali . . . . .	373
12.5	Jedinice i klase ideala . . . . .	380
12.6	Zadatci . . . . .	387
<b>13</b>	<b>Aproksimacija algebarskih brojeva</b>	<b>389</b>
13.1	Liouvilleov teorem . . . . .	389
13.2	Rothov teorem . . . . .	391
13.3	Hipergeometrijska metoda . . . . .	394
13.4	Aproksimacija kvadratnim iracionalnostima . . . . .	403
13.5	Separacija korijena polinoma . . . . .	408
13.6	Zadatci . . . . .	414

<b>14 Diofantske jednadžbe II</b>	<b>417</b>
14.1 Thueova jednadžba . . . . .	417
14.2 Tzanakisova metoda . . . . .	421
14.3 Linearne forme u logaritmima . . . . .	426
14.4 Baker-Davenportova redukcija . . . . .	431
14.5 LLL-redukcija . . . . .	436
14.6 Diofantove $m$ -torke . . . . .	440
14.7 Zadatci . . . . .	448
<b>15 Eliptičke krivulje</b>	<b>451</b>
15.1 Uvod u eliptičke krivulje . . . . .	451
15.2 Jednadžbe eliptičke krivulje . . . . .	458
15.3 Torzijska grupa . . . . .	471
15.4 Kanonska visina i Mordell-Weilov teorem . . . . .	483
15.5 Rang eliptičke krivulje . . . . .	490
15.6 Konačna polja . . . . .	504
15.7 Eliptičke krivulje nad konačnim poljima . . . . .	510
15.8 Primjena eliptičkih krivulja u kriptografiji . . . . .	518
15.9 Dokazivanje prostosti s pomoću eliptičkih krivulja . . . . .	527
15.10 Faktorizacija s pomoću eliptičkih krivulja . . . . .	531
15.11 Zadatci . . . . .	535
<b>16 Diofantski problemi i eliptičke krivulje</b>	<b>539</b>
16.1 Kongruentni brojevi . . . . .	539
16.2 Mordellova jednadžba . . . . .	541
16.3 Primjena faktorizacije u kvadratnim poljima . . . . .	543
16.4 Transformacija eliptičkih krivulja u Thueove jednadžbe . . . . .	548
16.5 Algoritam za rješavanje Thueove jednadžbe . . . . .	550
16.6 $abc$ slutnja . . . . .	556
16.7 Diofantove $m$ -torke i eliptičke krivulje . . . . .	560
16.8 Zadatci . . . . .	567
<b>Bibliografija</b>	<b>570</b>
<b>Indeks oznaka</b>	<b>591</b>
<b>Indeks pojmova</b>	<b>594</b>