

Obsah

1	Prvočísla	8
1.1	Prvočísel je nekonečně mnoho	8
1.2	Rozložení prvočísel	11
1.3	Mertensovy věty	16
1.4	Počty dělitelů	20
1.5	Eulerova funkce	23
2	Trocha algebry	29
2.1	Grupy, okruhy, tělesa - základní pojmy	29
2.2	Dělitelnost v oborech integrity	31
2.3	Okruhy polynomů	33
2.4	Konstrukce těles a tělesové automorfizmy	35
3	Něco o polynomech	41
3.1	Polynomy s koeficienty v $\mathbb{Q}$ a $\mathbb{Z}$	41
3.2	Cyklotomické polynomy	44
3.3	Symetrické polynomy	48
4	Algebraická číselná tělesa	53
4.1	Algebraická čísla, minimální polynom	53
4.2	Vlastnosti množiny algebraických čísel	55
4.3	Algebraická číselná tělesa	59
4.4	Izomorfizmy těles $\mathbb{Q}(\alpha)$	63
4.5	Tělesový polynom, norma, stopa	66
4.6	Příklady algebraických číselných těles	68
5	Diofantické rovnice	71
5.1	Kvadratická rezidua	71

5.2	Lineární diofantické rovnice	73
5.3	Pythagorejské trojice	75
5.4	Součet dvou čtverců	77
5.5	Součet čtyř čtverců	80
5.6	Pellova rovnice	82
6	Racionální aproximace reálných čísel	88
6.1	Fareyovy zlomky	88
6.2	Řetězové zlomky	91
6.3	Kontinuální polynomy	92
6.4	Aproximace sblíženými zlomky	94
6.5	Řetězový zlomek kvadratických čísel	101
6.6	Aplikace řetězových zlomků na diofantické rovnice	104
7	Transcendentní čísla	110
7.1	Liouvilleova čísla	111
7.2	Transcendentnost Eulerova čísla e	115
7.3	Transcendentnost čísla π	117
7.4	Řetězový zlomek Eulerova čísla e	120
8	Okruh celých čísel v číselném tělese	124
8.1	Algebraická celá čísla	124
8.2	Integrální báze okruhu celých čísel	126
8.3	Hledání integrální báze	131
8.4	Integrální báze v cyklotomických tělesech	135
9	Dělitelnost a faktorizace v okruhu celých čísel	139
9.1	Jednotky	139
9.2	Jednotky v kvadratických tělesech	140
9.3	Prvočísla, ireducibilní prvky, faktorizace	143
9.4	Faktorizace v kvadratických tělesech	148
10	Aplikace algebraických těles: Prvočíselné rozklady	153
10.1	Řešení diofantických rovnic	153
10.2	Lucasův–Lehmerův test prvočíselnosti	160

11 Aplikace algebraických těles v geometrii	165
11.1 Konstruovatelná čísla	166
11.2 Konstrukce pravidelného n -úhelníku	168
Literatura	175
Rejstřík	177