

OBSAH

Úvod	9
1. Předpoklady	10
1.1. Algoritmy a složitost	10
1.2. Komutativní algebra	11
1.3. Teorie čísel a abelovské grupy	16
2. Software	17
I. Základní obory a operace	19
3. Počítačová reprezentace dat	20
3.1. Základní datové typy	20
3.2. Datová reprezentace celých čísel	21
3.3. Datová reprezentace racionálních čísel	21
3.4. Datová reprezentace rozšíření těles konečného stupně	22
3.5. Datová reprezentace polynomů	22
3.6. Reprezentace obecných výrazů	23
4. Základní operace v oboru celých čísel	24
4.1. Školské algoritmy	25
4.2. Rychlejší násobení: metoda „rozděl a panuj“	28
4.3. Mocniny	31
4.4. Největší společný dělitel	32
4.5. Operace v oboru racionálních čísel	36
4.6. Operace v tělesech \mathbb{Z}_p	36
5. Základní operace s polynomy	39
5.1. Operace s polynomy	40
5.2. Operace v konečných tělesech a rozšířeních racionálních čísel	41
II. Modulární reprezentace a rychlé násobení	45
6. Zobecněná čínská věta o zbytcích	46
6.1. Čínská věta o zbytcích a interpolace	46
6.2. Modulární reprezentace	49
7. Algoritmy na čínskou větu o zbytcích	52
7.1. Lagrangeův algoritmus	52
7.2. Garnerův algoritmus	54
7.3. Sdílení tajemství	56
8. Fourierova transformace	57
8.1. Diskrétní Fourierova transformace	58
8.2. Rychlá Fourierova transformace	60
8.3. Primitivní odmocniny z jedné	61
9. Rychlé násobení polynomů	64
III. Newtonova metoda a rychlé dělení	69
10. Rychlé dělení polynomů	70
10.1. Algoritmus dělení	70
10.2. Výpočet inverzní mocninné řady	72
10.3. Aproximace zlomků	73
11. Kořeny obecných rovnic	75
11.1. Zužování intervalu	76
11.2. Newtonovy metody	77

IV. Největší společný dělitel	81
12. Posloupnosti polynomiálních zbytků	83
13. Rezultant a Sylvesterovo kritérium nesoudělnosti	88
14. Modulární algoritmus na výpočet NSD	93
14.1. Modulární algoritmus v $\mathbb{Z}[x]$	94
14.2. Modulární algoritmus pro polynomy více proměnných	99
V. Faktorizace	103
15. Bezčtvercová faktorizace	104
15.1. Bezčtvercová faktorizace v charakteristice 0	106
15.2. Bezčtvercová faktorizace nad konečnými tělesy	108
16. Faktorizace polynomů nad konečným tělesem	110
17. Faktorizace polynomů nad celými čísly	115
17.1. Pomocné algoritmy	116
17.2. Henselovo zdvihání	118
17.3. Kombinace faktorů	121
17.4. Berlekamp-Henselův algoritmus	123
18. Faktorizace polynomů více proměnných	125
18.1. Kroneckerův algoritmus	125
18.2. Analogie Berlekamp-Henselova algoritmu	127
VI. Gröbnerovy báze	131
19. Ideály v oborech polynomů více proměnných	132
19.1. Problém nalezení ideálu	132
19.2. Báze ideálu	134
19.3. Princip metody Gröbnerovýchází	135
20. Přepisování	136
20.1. Konvergentní grafy	137
20.2. Uspořádání termů	139
20.3. Přepisovací pravidla	140
21. Výpočet Gröbnerovy báze	143
21.1. Buchbergerův algoritmus	143
21.2. Redukované báze	147
22. Ideály, radikály a aplikace	149
22.1. Ideály	149
22.2. Radikály	150
22.3. Eliminace a řešení polynomiálních rovnic	152
22.4. Barvení grafů a dolní odhad složitosti	153
22.5. Automatické dokazování geometrických úloh	154
VII. Lenstra-Lenstra-Lovászův algoritmus	159
23. Gram-Schmidtova ortogonalizace	160
24. Mřížky	163
24.1. Základní vlastnosti	163
24.2. Dimenze 2	164
25. LLL-redukovaná báze a LLL algoritmus	167
26. Aplikace LLL redukce	174
26.1. Celočíslné vztahy mezi čísly	175
26.2. Diofantická aproximace	175

26.3. Faktorizace celočíselných polynomů	176
Rejstřík	179