

代数入门

2020年度版

中野 伸

(学习院大学・理学部・数学科)

目次

第1章	はじめに	1
1.1	不定方程式	1
1.2	ピタゴラス方程式	2
1.3	フェルマーの最終定理	3
1.4	有名な問題	3
第2章	整除関係	5
2.1	割り算と余り	5
2.2	約数・倍数	6
2.3	ユークリッドの互除法	7
第3章	最小値原理と数学的帰納法	9
3.1	最小値原理	9
3.2	最大公約数再論	11
第4章	素数と素因数分解の一意性	13
4.1	素数の定義	13
4.2	素数が無限個あること	15
4.3	ゼータ関数	16
第5章	整数の合同	17
5.1	合同式	17
5.2	法に関する逆元	19
第6章	合同式を解く	21
6.1	1次合同式	21
6.2	中国の剰余定理	23
第7章	剰余類と剰余環	25
7.1	剰余類	25
7.2	剰余類の和と積	26
7.3	剰余環の分解	27
7.4	中国の剰余定理再論	28

第 8 章	既約剰余類群とオイラー関数	29
8.1	既約剰余類群	29
8.2	オイラー関数	30
8.3	オイラー関数の積公式	31
8.4	オイラー関数の和公式	32
第 9 章	フェルマー, オイラーの定理	33
9.1	フェルマーの定理	33
9.2	フェルマーテスト	33
9.3	オイラーの定理	34
9.4	位数	35
第 10 章	暗号システム	37
10.1	暗号	37
10.2	Diffie-Hellman 鍵共有	37
10.3	RSA 公開鍵暗号	39
10.4	ハイブリッド暗号システム	40
第 11 章	平方剰余	41
11.1	平方剰余記号	41
11.2	平方剰余の相互法則, 補充法則	42
11.3	2次合同式	44
第 12 章	補充法則と相互法則の証明	45
12.1	補充法則の証明	45
12.2	ガウス和	45
12.3	もっとガウス和	47
12.4	相互法則の証明	48
第 13 章	補遺	49
13.1	孫子算経	49
13.2	命題 8.5 の証明	50
13.3	補題 12.7 の証明	50

間違いを見つけたら……, ひそかにそっと連絡して下さい…….

中野 伸 <shin.nakano@gakushuin.ac.jp>

白いページ