

# 代数入门

2022年度版

中野 伸

(学习院大学・理学部・数学科)

# 目次

<b>第1章</b>	<b>はじめに</b>	<b>1</b>
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
<b>第2章</b>	<b>整除関係</b>	<b>5</b>
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
<b>第3章</b>	<b>最小値原理と数学的帰納法</b>	<b>9</b>
3.1	最小値原理	9
3.2	最大公約数再論	11
<b>第4章</b>	<b>素数と素因数分解の一意性</b>	<b>13</b>
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
<b>第5章</b>	<b>整数の合同</b>	<b>17</b>
5.1	合同式	17
5.2	法に関する逆元	19
<b>第6章</b>	<b>合同式を解く</b>	<b>21</b>
6.1	1次合同式	21
6.2	中国の剰余定理	23
<b>第7章</b>	<b>剰余類と剰余環</b>	<b>25</b>
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

<b>第 8 章</b>	<b>既約剰余類群とオイラー関数</b>	<b>29</b>
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
<b>第 9 章</b>	<b>フェルマー, オイラーの定理</b>	<b>33</b>
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
<b>第 10 章</b>	<b>暗号システム</b>	<b>37</b>
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
<b>第 11 章</b>	<b>平方剰余</b>	<b>41</b>
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
<b>第 12 章</b>	<b>補充法則と相互法則の証明</b>	<b>45</b>
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
<b>第 13 章</b>	<b>補遺</b>	<b>49</b>
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……, そっと連絡して下さい…….

中野 伸 <shin.nakano@gakushuin.ac.jp>

白いページ