代 数 入 門

2026 年度版

中野　伸

（学習院大学・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　一次合同式 **21**
6.1　合同式を解く 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 オイラーの定理 33
9.3 ちょっとだけ精密化 35
9.4 フェルマーテスト 36

第 10 章 位数と原始根 **37**
10.1 位数 37
10.2 多項式に関する注意 39
10.3 原始根 40

第 11 章 暗号システム **41**
11.1 暗号 41
11.2 ディフィー・ヘルマン鍵共有 41
11.3 RSA 公開鍵暗号 43
11.4 ハイブリッド暗号システム 44

第 12 章 平方剰余 **45**
12.1 平方剰余記号 45
12.2 平方剰余の相互法則，補充法則 46
12.3 二次合同式 48

第 13 章 補充法則と相互法則の証明 **49**
13.1 補充法則の証明 49
13.2 ガウス和 49
13.3 もっとガウス和 51
13.4 相互法則の証明 52

第 14 章 相互法則の別証明 **53**
14.1 相互法則の別証明 53

第 15 章 補遺 **57**
15.1 孫子算経 57
15.2 命題 8.5 の証明 58
15.3 奇素数べきを法とする原始根 58
15.4 補題 13.6 の証明 60

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>