

ЗМІСТ

Передмова	8
Розділ 1. Елементи теорії чисел	9
1.1. Числові множини.....	9
1.1.1. Конструктивне означення множини натуральних чисел.....	9
1.1.2. Аксиоматика множини цілих чисел.....	12
1.1.3. Аксиоматика множини раціональних чисел	12
1.1.4. Аксиоматика множини дійсних чисел.....	14
1.2. Приклади застосування аксіоми індукції.....	18
1.3. Арифметика натуральних і цілих чисел.....	19
1.3.1. Теорема про ділення з остачею в кільці цілих чисел \mathbb{Z}	19
1.3.2. Теорія подільності в кільці цілих чисел. Прості і складені числа.....	20
1.3.3. Факторизація. Основна теорема арифметики та її наслідки.....	21
1.3.4. Найбільший спільний дільник. Алгоритм Евкліда.....	21
1.3.5. Співвідношення Безу. Діофантові рівняння.....	22
1.4. Ланцюгові дроби	24
1.4.1. Поняття ланцюгового дроби.....	24
1.4.2. Підхідні дроби ланцюгового дроби	26
1.4.3. Застосування ланцюгових дробів.....	27
1.4.4. Приклади розв'язування задач	28
1.5. Числові функції та їх властивості	30
1.5.1. Арифметична функція та мультиплікативна арифметична функція	31
1.5.2. Обчислення значень функцій $\tau(n)$, $\sigma(n)$	34
1.5.3. Обчислення значень функції Ейлера	36
1.6. Застосування функції Ейлера.....	38
1.6.1. Формула Гауса	38
1.6.2. Теореми Ейлера та Ферма.....	39
1.7. Функція Мебіуса та її властивості	40

Розділ 2. Конгруенції	41
2.1. Конгруенції і кільця класів лишків	41
2.1.1. Означення конгруенцій та їхні найпростіші властивості.....	41
2.1.2. Застосування властивостей конгруенцій	42
2.1.3. Класи лишків за даним модулем	43
2.1.4. Повна та зведена системи лишків за модулем m	44
2.1.5. Приклади розв'язування задач.....	45
2.2. Лінійні конгруенції з одним невідомим та їх розв'язування	49
2.2.1. Перетворення конгруенцій.....	49
2.2.2. Конгруенції 1-го степеня з одним невідомим	49
2.2.3. Способи розв'язування конгруенції 1-го степеня.....	50
2.2.4. Розв'язування систем конгруенцій.....	51
2.2.5. Приклади розв'язування задач.....	52
2.3. Конгруенції вищих степенів	57
2.3.1. Лишки та нелишки вищих степенів	58
2.3.2. Символ Лежандра та його властивості.....	58
2.3.3. Приклади розв'язування конгруенцій другого степеня.....	60
2.4. Порядок числа і класу лишків за модулем	62
2.4.1. Первісні корені, їх існування та кількість за простим модулем	62
2.4.2. Приклади розв'язування задач.....	64
2.5. Індеси за простим модулем. Двочленні конгруенції за простим модулем. Таблиці індесів та їх застосування	65
2.5.1. Приклади розв'язування задач	66
Розділ 3. Алгебраїчні структури	70
3.1. Основні поняття теорії груп.....	70
3.1.1. Поняття про бінарну операцію	71
3.1.2. Групи перетворень	73
3.1.3. Групи	74
3.1.4. Суміжні класи. Теорема Лагранжа	76
3.1.5. Внутрішній автоморфізм.....	77
3.1.6. Нормальні підгрупи	78

3.1.7. Факторгрупи.....	79
3.2. Групи та їх морфізми	81
3.2.1. Огляд деяких теоретико-групових понять та прикладів груп	81
3.2.2. Теорема Келлі	82
3.2.3. Прямий добуток груп	82
3.2.4. Теореми про гомоморфізми груп та підгруп.....	84
3.2.5. Комутант	84
3.2.6. Розв'язні групи.....	85
3.3. Основні поняття теорії кілець	86
3.3.1. Означення кільця та найпростіші наслідки з аксіом	86
3.3.2. Приклади кілець	89
3.3.3. Гомоморфізми та ізоморфізми кілець	90
3.3.4. Вкладення кільця в кільце з одиницею.....	91
3.3.5. Прямі добутки та прямі суми кілець.....	91
3.4. Ідеали та фактор-кільця	92
3.4.1. Означення ідеалів. Головні та скінченно породжені ідеали.....	92
3.4.2. Ідеали в полі.....	94
3.4.3. Фактор-кільця за ідеалами	94
3.4.4. Теореми про гомоморфізм кілець	95
3.4.5. Основні операції над ідеалами	96
3.4.6. Прості і максимальні ідеали	97
3.4.7. Деякі класи кілець з умовами на їх ідеали. Нетерові та артїнові кільця.....	98
3.4.8. Теорема Гільберта про базу	99
3.5. Скінченні поля та їх розширення.....	100
3.5.1. Кількість елементів скінченного поля.....	101
3.5.2. $GF(q)$ – поле розкладу многочлена $X^q - X$ та підполя скінченного поля.....	102
3.5.3. Конструкції скінченних полів	103
3.5.4. Мультиплікативна структура скінченного поля.....	107

Розділ 4. Раціональні точки на еліптичних кривих	109
4.1. Еліптичні криві в криптографії.....	109

4.1.1. Способи побудови еліптичних кривих.....	109
4.1.2. Властивості множини точок $E_p(a, b)$	115
4.1.3. Дискретне логарифмування на еліптичній кривій.....	117
4.2. Групові операції на еліптичних кривих.....	117
4.2.1. Основні типи еліптичних кривих	117
4.2.1.1. Еліптичні криві у формі Веєрштрасса.....	117
4.2.1.2. Криві Якобі	119
4.2.1.3. Криві Гессе.....	120
4.2.1.4. Криві Гаффа	121
4.2.1.5. Криві Едвардса	122
4.2.1.6. Еліптичні криві Лежандра-Лау	123
4.2.2. Висновки.....	124
Розділ 5. Методи та алгоритми розв’язування типових задач	125
5.1. Типові задачі з розділу 1 “Елементи теорії чисел”	125
5.1.1. Арифметика натуральних і цілих чисел.....	125
5.1.2. Ланцюгові дроби	128
5.1.3. Числові функції та їх властивості.....	130
5.1.4. Тести для перевірки знань з розділу 1.....	130
5.1.5. Відповіді до тестових завдань з розділу 1	136
5.2. Типові задачі з розділу 2 “Конгруенції”	136
5.2.1. Конгруенції.....	136
5.2.2. Кільця класів лишків.....	138
5.2.3. Лінійні конгруенції з одним невідомим.....	139
5.2.4. Методи розв’язування систем лінійних конгруенцій	142
5.2.5. Конгруенції вищих степенів. Квадратичні лишки. Порядок числа і класу лишків за модулем. Індокси. Двочленні конгруенції.....	145
5.2.6. Тести для перевірки знань з розділу 2.....	148
5.2.7. Відповіді до тестових завдань з розділу 2	152
5.3. Типові задачі з розділу 3 “Алгебраїчні структури”	153
5.3.1. Властивості підстановок. Групи	153

5.3.2. Кільця. Скінченні поля.....	154
5.3.3. Тести для перевірки знань з розділу 3	158
5.3.4. Відповіді до тестових завдань з розділу 3.....	166
5.4. Розв'язування задач з розділу IV	166
5.4.1. Особливі точки кривих вищих степенів.....	166
5.4.2. Групові операції на еліптичних кривих.....	167
5.4.3. Тести для перевірки знань з розділу 4	169
5.4.4. Відповіді до тестових завдань з розділу 4.....	173
Розділ 6. Умови індивідуальних розрахункових завдань.....	174
6.1. Розрахункові завдання з розділу 1.....	174
6.2. Розрахункові завдання з розділу 2	176
6.3 Розрахункові завдання з розділу 3.....	182
6.4. Розрахункові завдання з розділу 4.....	184
Список літератури	188