

О. І. Клесов

**ЕЛЕМЕНТАРНА
ТЕОРІЯ ЧИСЕЛ ТА
ЕЛЕМЕНТИ КРИПТОГРАФІЇ**

ПІДРУЧНИК

Рекомендовано Вченою радою НТУУ “КПІ”
як підручник для студентів вищих навчальних закладів,
які навчаються за спеціальністю “математика та статистика”

⟨⟨ТВіМС⟩⟩

Київ

2016

УДК 519.21
ББК 22.171
К–18

Рецензенти:

В. В. Гавриленко — доктор фізико-математичних наук, професор, завідувач кафедри інформаційних систем і технологій Національного транспортного університету

П. В. Задерей — доктор фізико-математичних наук, професор, завідувач кафедри вищої математики Київського університету технологій та дизайну

Затверджено Науковою радою Національного технічного університету “КПІ” (протокол № 8 від 30.06.2016 р.) як підручник для студентів вищих навчальних закладів, які навчаються за спеціальністю “111. Математика та статистика”

Клесов О. І.

**К–18 ЕЛЕМЕНТАРНА ТЕОРІЯ ЧИСЕЛ ТА
ЕЛЕМЕНТИ КРИПТОГРАФІЇ: Підручник. — К.:
ТВіМС, 2016. — 412 стор.**

Підручник містить відомості з теорії чисел, які необхідні для оволодіння елементами криптографії, а також класичні та сучасні методи шифрування інформації включно з методами RSA, Ель-Гамала, цифрового підпису, які входять до навчального плану освітньо-кваліфікаційного рівня “бакалавр” зі спеціальності “Математика та статистика”.

ББК 22.171
УДК 519.21

ISBN 978–966–8725–11–1

© О. І. Клесов

Зміст

ПЕРЕДМОВА

Глава 1. Зв'язок між теорією чисел та криптографією	1
1.1. “Апологія математика”	1
1.1.1. Чи правий Харді?	2
1.1.2. Чи існують застосування математики?	3
1.1.3. Чи існують застосування теорії чисел?	3
1.2. Як кодують повідомлення	4
1.2.1. Математичні шифри	9
1.3. Перевірка числа на простоту	10
1.4. Решето Ератосфена	12
1.5. Кілька відомих шифрів	16
1.5.1. Шифр перестановки	16
1.5.2. Рандомізований матричний шифр	17
1.5.3. Азбука Брайля	18
1.5.4. Азбука Морзе	19
1.6. Контрольні питання	20
1.7. Задачі	20
1.8. Біографії	27
Глава 2. Шифр Цезаря	37
2.1. Код клавіатури	38
2.2. Шифр Цезаря	38
2.2.1. Використання чисел у шифрі Цезаря	40
2.3. Подільність натуральних чисел	42

2.3.1. Ділення з остачею	43
2.4. Властивості конгруенції	44
2.5. Найбільший спільний дільник	46
2.6. Прості числа та основна теорема арифме- тики	46
2.6.1. Закон розподілу простих чисел	49
2.7. Шифр Віженера	50
2.8. Шифр Вернама	53
2.9. Контрольні питання	54
2.10. Задачі	55
2.11. Біографії	61
Глава 3. Мультиплікативні шифри	66
3.1. Означення мультиплікативних шифрів	66
3.1.1. M_2 -шифр	67
3.1.2. Дешифрування M_2 -шифру	68
3.1.3. Шифр M_3	69
3.2. Обернені числа в арифметиці за модулем ...	70
3.3. Властивості шифру $M_{a,n}$	72
3.3.1. Дешифрування $M_{a,n}$ шифру	72
3.3.2. Криптоаналіз M_a шифру	72
3.3.3. Алгебраїчний спосіб дешифрування	73
3.3.4. Для яких a існують M_a шифри	74
3.3.5. Інші алфавіти	75
3.4. Контрольні питання	77
3.5. Задачі	78
3.6. Біографії	86
Глава 4. Алгоритми Евкліда	88
4.1. Алгоритм Евкліда знаходження найбільшого спільного дільника	89

4.2. Знаходження оберненого числа в арифметиці за модулем	92
4.2.1. Побудова оберненого за модулем	94
4.3. Розширений алгоритм Евкліда	98
4.4. Контрольні питання	101
4.5. Задачі	102
4.6. Біографії	107
Глава 5. Шифр Хілла	110
5.1. Дешифрування шифру Хілла	111
5.2. Системи лінійних конгруенцій	112
5.2.1. Одне рівняння	112
5.2.2. Система двох рівнянь	113
5.3. Дешифрування шифру Хілла: закінчення .	115
5.3.1. Блоки іншого розміру	117
5.4. Криптоаналіз шифру Хілла	118
5.5. Системи лінійних рівнянь за модулем	118
5.6. Шифр Плейфера	122
5.7. Контрольні питання	125
5.8. Задачі	126
5.9. Біографії	134
Глава 6. Лінійні шифри	136
6.1. Дешифрування лінійного шифру	137
6.2. Скільки існує лінійних шифрів?	138
6.2.1. Випадок загального n	139
6.3. Функція Ойлера	140
6.3.1. Формула включення/виключення	141
6.3.2. Загальна формула для функції Ойлера ...	143
6.4. Теорема Ойлера	145
6.4.1. Обчислення оберненого за модулем	146

6.4.2. Мала теорема Ферма	147
6.5. Таблиця перших значень функції Ойлера .	147
6.6. Контрольні питання	148
6.7. Задачі	149
6.8. Біографії	154
Глава 7. Криптоаналіз лінійних шифрів	156
7.1. Алгебраїчний метод для $L_{a,b}$ шифрів	156
7.1.1. Як розв'язувати лінійні рівняння у модульній арифметиці	156
7.1.2. Як розв'язувати системи лінійних рівнянь у модульній арифметиці	158
7.2. Частотний аналіз	159
7.3. Надійність лінійних шифрів	163
7.3.1. Принцип Керкхоффа	164
7.3.2. Принцип складності обчислень	164
7.3.3. Лист Джона Неша	165
7.3.4. Найбільш загадковий рукопис	166
7.3.5. Час, потрібний для зламу лінійного шифру	167
7.4. Ще раз про знаходження оберненого за модулем	169
7.5. Контрольні питання	170
7.6. Задачі	171
7.7. Біографії	178
Глава 8. Експоненціальні шифри	180
8.1. Особливості експоненціального шифру	180
8.1.1. Яким має бути n	181
8.1.2. Експоненціальний шифр не є підстановкою	181
8.2. Властивість конгруенцій, необхідна для експоненціальних шифрів	183

8.3. Дешифрування експоненціального шифру .	183
8.3.1. Обчислення показника кореня	184
8.3.2. Обчислення показника кореня, коли $n = p$.	185
8.3.3. Обчислення показника кореня, коли $n = pq$	186
8.3.4. Як створити свій експоненціальний код . . .	188
8.4. Швидке піднесення до степеня	189
8.5. Швидке піднесення до степеня за модулем	190
8.5.1. Бінарне представлення	192
8.6. Контрольні питання	194
8.7. Задачі	196
8.8. Біографії	201

Глава 9. Криптоаналіз експоненціальних шифрів 202

9.1. Дешифрування у випадку коли степінь та модуль відомі	202
9.2. Дешифрування у випадку коли показник або модуль невідомі	205
9.3. Надійність експоненціальних шифрів	208
9.3.1. Метод факторизації Крайчика	211
9.4. Односторонні функції	214
9.4.1. Односторонні функції з секретом	214
9.4.2. Дискретний логарифм	215
9.4.3. Захист пароля	216
9.4.4. Алгоритм Шенкса	217
9.5. Контрольні питання	219
9.6. Задачі	221

Глава 10. Криптосистеми з відкритим ключем 229

10.1. Головоломки Меркла	230
------------------------------------	-----

10.2. Метод В. Діффі та М. Хеллмана	230
10.3. Шифр RSA	232
10.3.1. Що таке шифр RSA	232
10.3.2. Відкритий та приватний ключі для RSA ..	234
10.3.3. Надійність RSA	235
10.3.4. Початок історії RSA	236
10.3.5. Припущення щодо RSA	238
10.3.6. Інший спосіб запису RSA	239
10.4. Доведення алгоритму RSA	240
10.5. Атаки на RSA	241
10.5.1. Факторизація n якщо відоме $\phi(n)$	242
10.5.2. Факторизація n , якщо $ p - q $ є малим	242
10.6. Задача про рюкзак в криптографії	244
10.6.1. Задача про рюкзак для суперзростаючих пос- лідовностей	244
10.6.2. Криптосистема, основана на задачі про рюкзак	245
10.7. Метод Ель-Гамалія	247
10.7.1. Примітивний корінь числа	248
10.7.2. Криптосистема Ель-Гамалія	250
10.8. Контрольні питання	255
10.9. Задачі	256
10.10. Біографії	263
Глава 11. Цифровий підпис	269
11.1. Метод RSA для цифрового підпису	269
11.2. Дайджест	273
11.2.1. Хеш функції	275
11.3. Сліпий цифровий підпис	277
11.3.1. Вимоги до схеми сліпого підпису	278
11.3.2. Доведення алгоритму 1	280

11.4.	Застосування схеми сліпого підпису	281
11.4.1.	Електронні гроші	281
11.4.2.	Таємне голосування	284
11.5.	Цифровий підпис для схеми Ель-Гамалія .	287
11.5.1.	Невдала хеш функція	290
11.5.2.	Атака, якщо j є відомим	291
11.5.3.	Атака, якщо j повторюється	291
11.6.	Розподілення секретів	292
11.7.	Контрольні питання	296
11.8.	Задачі	297
11.9.	Біографії	305
Глава 12. Перевірка чисел на простоту		306
12.1.	Кілька відомих способів перевірки чисел на простоту	307
12.1.1.	Формула Мілса	307
12.1.2.	Критерій Вілсона	308
12.2.	Псевдопрості числа	309
12.3.	Числа Кармайкла	313
12.3.1.	Найменше з чисел Кармайкла	314
12.3.2.	Необмеженість множини чисел Кармайкла	315
12.3.3.	Теорема Корселта	315
12.4.	Тест Соловея–Штрассена	317
12.4.1.	Тест Соловея–Штрассена	318
12.4.2.	Оптимальність тесту Соловея–Штрассена	321
12.4.3.	Обґрунтування тесту Соловея–Штрассена	323
12.4.4.	Кілька ітерацій тесту Соловея–Штрассена	324
12.5.	Тест Міллера	328
12.6.	Тест Рабіна–Міллера	332
12.6.1.	Рандомізований алгоритм	333
12.6.2.	PRIMES is in P	336

12.7. Контрольні питання	336
12.8. Задачі	338
12.9. Біографії	345
Глава 13. Теорема Чебишова	351
13.1. Асимптотика кількості простих чисел	357
13.1.1. Про доведення теореми про прості числа .	357
13.2. Постулат Бертрана	358
13.2.1. Теорема Райта	363
13.3. Асимптотика функції Чебишова	364
13.4. Асимптотика n -ого простого числа	366
13.5. Контрольні питання	369
13.6. Задачі	372
13.7. Біографії	377
СПИСОК ЛІТЕРАТУРИ	385
ПРЕДМЕТНИЙ ПОКАЖЧИК	387
СПИСОК ПОЗНАЧЕНЬ	393

Передмова

Розкажи мені — я забуду.

Покажи мені — я запам'ятаю.

Зроби разом зі мною — я навчусь.

Конфуцій

В основу цього підручника покладено курс лекцій з такою ж назвою, який автор викладає на фізико-математичному факультеті Національного технічного університету України “Київський політехнічний інститут”.

Назва курсу лекцій “*Елементарна теорія чисел та елементи криптографії*” правильно відображає його зміст: він дійсно містить лише найпростіші теми з теорії чисел та сучасної криптографії.

При написанні цього підручника автор не мав на меті викласти в повному обсязі (елементарну) теорію чисел або (елементарну) криптографію. Натомість мета полягала у тому, щоб показати, що навіть прості факти з теорії чисел можуть бути корисними у сучасних застосуваннях та у доступній формі описати такі застосування у криптографії.

Автор намагався представити матеріал в першу чергу для студентів, які вивчають математику. Тому в підручнику доведено багато простих, але необхідних фактів з елементарної теорії чисел, що є обов'язковою складовою освіти

математиків. Можливо, іншим студентам, які спеціалізуються, наприклад, у галузі захисту інформації, деякі з доведень будуть здаватися зайвими.

Майже всі теми, що увійшли до підручника, є достатньо простими (принаймні для математиків). Проте це не означає, що всі математичні методи криптографії (навіть ті, які представлені в цьому підручнику) є простими і легко доступними читачам без належної підготовки. Прикладом може служити глава 13, де розглянуто асимптотику кількості простих чисел.

Кілька слів до викладачів. Кожна з глав містить більше матеріалу, ніж лектор зможе викласти в нормальному темпі за 2 академічні години. Залежно від навчальної програми додатковий матеріал кожної глави можна пропонувати студентам для самостійної роботи або викладати на наступному занятті. Мені здається, що для того, щоб викласти весь матеріал цього підручника, вистачить 18–20 лекційних занять.

Уявлення про теми, представлені в підручнику, дає наступний перелік:

теми з криптографії

лінійні шифри
 мультиплікативні шифри
 шифр Хілла
 експоненціальні шифри
 метод RSA
 криптосистема Ель-Гамала
 “рюкзачна” криптосистема
 цифровий підпис

теми з теорії чисел

арифметика за модулем
 обернені за модулем
 алгоритми Евкліда
 функція Ойлера
 перевірка чисел на простоту
 системи конгруенцій
 примітивні корені
 асимптотика простих чисел

Саме ці теми складають семестрову навчальну програму курсу на фізико-математичному факультеті КПІ.

В залежності від вподобань лектора курс лекцій можна доповнити однією або кількома наступними темами, які також досить детально викладено в підручник: системи конгруенцій, примітивні корені, рюкзачні системи, алгоритми факторизації натуральних чисел тощо. Крім цього, в підручнику обговорюються також інші застосування, які не мають прямого відношення до теорії чисел або криптографії, але які використовують ті ж результати та аналогічні протоколи, а саме: сліпий підпис, таємне голосування, розподілені секрети, електронні гроші тощо.

Хоча назви багатьох глав є “криптографічними”, вони більше ніж наполовину складаються з результатів теорії чисел. Наприклад, назвою глави 2 є “*Шифр Цезаря*” хоча в ній, разом з шифрами Цезаря, Вернама та Віженера, розповідається також і про “*Подільність натуральних чисел*”, “*Ділення з остачею*”, “*Властивості конгруенції*”, “*Найбільший спільний дільник*”, “*Прості числа та основна теорема арифметики*”, “*Закон розподілу простих чисел*”.

Наприкінці кожної глави є розділ “*Контрольні питання*”, які можна використати для оперативної перевірки рівня оволодіння матеріалом даної глави. Іншою важливою складовою кожної глави є задачі, яких достатньо і для практичних занять, і для домашньої роботи. Приблизно половина задач відноситься до теорії чисел, а інша — до криптографії. Виключенням є глави 11 та 13, де задач з теорії чисел 0% та 100% відповідно.

Всі формули і форматування підручника здійснено за допомогою програми \TeX , автором якої є відомий американський математик Дональд Кнут. Ця програма зараз вва-

жається стандартним інструментом для підготовки математичних публікацій і тому нею користуються майже всі математики в усьому світі. Набагато менше відомі інші чудові властивості $\text{T}_{\text{E}}\text{X}'\text{y}$, які нагадують засоби інших мов програмування для комп'ютерів. Майже всі обчислення, представлені в підручнику, виконано за допомогою макросів, написаних мною засобами $\text{T}_{\text{E}}\text{X}'\text{y}$. Це дозволило мені під час підготовки цього підручника залишатись в комфортному “середовищі” $\text{T}_{\text{E}}\text{X}'\text{a}$.

Кілька слів до студентів. В тексті підручника багато позначок типу ①, які рекомендують читачеві подумати над певним питанням. Питання не складні, але читачу важливо знайти відповіді на кожен з них, щоб зрозуміти міркування автора. Саме ці питання складають розділ “Контрольні питання” в кінці кожної глави.

Твердження та формули в кожній главі нумеруються за допомогою одного числа, наприклад в главі 8 є “теорема 1” і протягом цієї глави я посилаюсь на неї як на “теорему 1”. Якщо ж вираз “теорема 8.1” зустрічається в іншій главі, то це означає, що автор посилається на “теорему 1 з глави 8”. Аналогічне правило стосується номерів інших типів тверджень, а також формул.

В кінці кожної глави наведено вправи, які необхідно виконати під час практичного заняття в аудиторії або вдома. Я вважаю, що гарною стратегією для студентів є повторення матеріалу останньої лекції перед черговим практичним заняттям, а також перед черговою лекцією. Поганою ж стратегією є намагання відкласти оволодіння матеріалом

¹Це порада автора читачу здійснити певну дію.

лекцій на період безпосередньої підготовки до іспиту. ②

В кінці підручника на стор. 385–386 наведено перелік (далекий від повного) посилань на інші літературні джерела, якими я користався під час написання свого підручника або які я рекомендую для подальшого вивчення матеріалу. Для бажаючих розширити свої знання з теорії чисел я рекомендую підручники [3] або [18], [20] (більш складні питання обговорюються в [17]). Дружніми до читача підручниками з криптографії я вважаю [9] або [10], а також [15] та [21]. Багато цікавих історичних відомостей про криптографію міститься в [8]. Алгоритмічні питання теорії чисел та криптографії обговорюються в [13]. Додаткові задачі з криптографії можна знайти в [6] та [11].

Кілька загальних зауважень. Автор не вважає правильним, що надто багато розділів з теорії чисел, теорії графів, алгебри або дискретної математики “відносяться” до комп’ютерних наук або так званої “прикладної математики”. Незрозумілою є й поведінка самих математиків, які добровільно відмовляються від цих розділів на підставі їх “занадто прикладного спрямування”.

Неприродний (або “віртуальний”, якщо вживати сучасний сленг) поділ на фундаментальну та прикладну науку існує не тільки в математиці і з’явився він не зараз. У часи І. Ньютона (XVII сторіччя) такого поділу ще не існувало. Через 300 років після Ньютона в своїй доповіді на Міжнародному симпозіумі з планування науки у 1959 році

²А тим більше до моменту безпосередньої відповіді на іспиті!

П. Л. Капіца сказав:

“... У зв'язку із зростанням масштабів наукової роботи відбувається поділ науки на фундаментальну і прикладну. Я думаю, що цей поділ багато в чому слід вважати штучним, і важко вказати точку, де кінчається фундаментальна і починається прикладна наука...”

Таким чином, у другій половині ХХ сторіччя вже існував “штучний” (за висловлюванням Капіци) поділ науки на фундаментальну та прикладну складові. Але ще за сто років до Капіци, Луї Пастер, якого важко запідозрити у зайвій схильності до теоретичних досліджень, був більш категоричним у своїх висловлюваннях:

“... Не існує жодних “прикладних наук”; є тільки одна НАУКА та її плоди — як дерево й плоди, ним породжені...”

Таким чином, в ХІХ сторіччі вчені вже дискутували з приводу поділу науки на дві складові. Мабуть неприродний поділ на фундаментальні та прикладні науки виник раніше, можливо у ХVІІІ сторіччі.

Правильним, на думку автора, шляхом розвитку математики є генерація математичних ідей математиками і використання ними ж цих ідей для розв'язання практичних задач разом із спеціалістами зі сміжних галузей.

Варто також зазначити, що в математиці існують задачі, які самі математики вважають важливими, але інші спеціалісти з цим не погоджуються. Захопленість математиків абстрактними конструкціями та теоріями може навіть стати приводом для глузування з боку нематематиків. Тому одним з завдань, які стоять перед сучасними математиками,

є пошук порозуміння з іншими вченими шляхом пояснення актуальності своїх досліджень.

У цьому зв'язку характерною є позиція видатного російського математика В. І. Арнольда стосовно доведення великої теореми Ферма, яка протягом більше трьох століть не піддавалась розв'язанню. Весь цей час вона приваблювала майже кожного з математиків, але жодному з них не вдавалося її підкорити до 1994 року, коли Ендрю Вайлс показав, що гіпотеза Ферма є вірною. Більшість математиків вважали його результат одним з найвидатніших у ХХ сторіччі. З цього приводу В. І. Арнольд писав, що галас, здійснений навколо доведення великої теореми Ферма, може привести до припинення фінансування цієї науки урядами і суспільством, оскільки на цьому прикладі стає зрозумілим, якою “непотрібною” діяльністю займаються математики.

Якщо знизити полемічний запал В. І. Арнольда й викласти його висловлювання у більш зваженому вигляді, то можливою інтерпретацією його слів буде така: математики повинні представляти свої результати у публічній сфері, причому таким чином, щоб вони були зрозумілими широкому загалу, в тому числі й керівникам, від яких залежить фінансування науки.

В. І. Арнольд вважає, що це зробити можна й це завдання є здійсненним, оскільки

“... справжня математика геометрична й сильна зв'язками з фізикою ...”

Інша точка зору, яка належить видатному англійському математику Г. Харді і з якою автор цього підручника полемізує у главі 1, полягає в тому, що справжня математика

не має нічого спільного з застосуваннями, а ті формули, що використовуються для застосувань, не є математикою.

Схожі думки висловлював інший видатний математик Давід Гільберт на початку XX сторіччя: він вважав, що математика не мала, не має і ніколи не буде мати жодних застосувань.

Екстремальна точка зору належить сучасному російському математику Ю. І. Маніну, який працює в Німеччині: він вважає, що математика потрібна лише для того, щоб відволікати розумних людей від інших зайнятть, які можуть нашкодити людству (наприклад, винаходами нових видів зброї).

Цю передмову я хочу завершити, навівши слова трьох видатних вчених, які додержуються іншої точки зору, ніж Харді, Гільберт чи Манін.

“ ... Не існує нічого більш практичнішого, ніж хороша теорія ... ”

Людвіг Больцман

“ ... Той, хто захоплюється практикою без науки, нагадує керманіча, який ступив на корабель без керма та компаса: він ніколи не знає, куди пливе ... ”

Леонардо да Вінчі

“ ... Наука повинна бути найбільш піднесеним втіленням патріотизму, оскільки той народ буде завжди першим, який випередить інших в області розумової діяльності ... ”

Луї Пастер

Ці промовисті цитати краще, ніж мої власні слова, пояснюють мою позицію.

Автор