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-Гамаля, 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

Зміст

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	**теми з теорії чисел**
лінійні шифри	арифметика за модулем
мультиплікативні шифри	обернені за модулем
шифр Хілла	алгоритми Евкліда
експоненціальні шифри	функція Ойлера
метод RSA	перевірка чисел на простоту
криптосистема Ель-Гамаля	системи конгруенцій
“рюкзачна” криптосистема	примітивні корені
цифровий підпис	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 TEX'у, які нагадують засоби інших мов програмування для комп'ютерів. Майже всі обчислення, представлені в підручнику, виконано за допомогою макросів, написаних мною засобами TEX'у. Це дозволило мені під час підготовки цього підручника залишатись в комфортному "середовищі" TEX'а.

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 кожну 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

[1] Це 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

[2] А 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 XX 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 XIX сторіччі вчені вже дискутували з приводу поділу науки на дві складові. Мабуть неприродний поділ на фундаментальні та прикладні науки виник раніше, можливо у XVIII 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 XX 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 Ґ. 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. Манінy, який працює в Німеччині: він вважає, що математика потрібна лише для того, щоб відволікати розумних людей від інших зайнять, 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 ... ”
>
> Людвіґ Больцман

> “ ... Той, хто захоплюється практикою без науки, нагадує керманича, 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