

Міністерство освіти і науки України
Харківський національний університет імені В. Н. Каразіна

ФАКТОРИЗАЦІЯ ЦІЛИХ ЧИСЕЛ

Методичні рекомендації
до лабораторної роботи з дисципліни «Теорія чисел, груп, полів, кілець»

для студентів
спеціальності 125 «Кібербезпека»

УДК 511.17

Ф 18

Рецензенти:

О. В. Лемешко – доктор технічних наук, професор, завідувач кафедри інфоко-мунікаційної інженерії імені В. В. Поповського Харківського національного університету радіоелектроніки;

О. Г. Толстолузька – доктор технічних наук, старший науковий співробітник, професор кафедри теоретичної та прикладної системотехніки факультету комп'ютерних наук Харківського національного університету імені В. Н. Каразіна.

*Затверджено до друку рішенням Науково-методичної ради
Харківського національного університету імені В. Н. Каразіна
(протокол № 5 від 10 червня 2021 року)*

Факторизація цілих чисел : методичні рекомендації до лабораторної роботи з
Ф 18 дисципліни «Теорія чисел, груп, полів, кілець» для студентів спеціальності 125 «Кібербезпека» / уклад. О. О. Кузнецов, М. О. Полуяненко, О. О. Полуяненко, Ю. М. Рябуха. – Харків : ХНУ імені В. Н. Каразіна, 2021. – 36 с.

Методичні рекомендації щодо факторизації цілих чисел розроблено для студентів факультету комп'ютерних наук за спеціальністю «Кібербезпека». Метою даних методичних рекомендацій до лабораторної роботи з дисципліни «Теорія чисел, груп, полів, кілець» є ознайомлення з основними способами факторизації цілих чисел, практична реалізація деяких алгоритмів і оволодіння найбільш ефективним програмним пакетом з факторизації цілих чисел.

УДК 511.17

© Харківський національний університет
імені В. Н. Каразіна, 2021

© Кузнецов О. О., Полуяненко М. О.,
Полуяненко О. О., Рябуха Ю. М., уклад., 2021

© Дончик І. М., макет обкладинки, 2021

Навчальне видання

Кузнецов Олександр Олександрович

Полуяненко Микола Олександрович

Полуяненко Ольга Олександрівна

Рябуха Юрій Миколайович

Факторизація цілих чисел

Методичні рекомендації до лабораторної роботи з дисципліни «Теорія чисел, груп, полів, кілець»
для студентів спеціальності 125 «Кібербезпека»

Коректор *О. В. Анцибора*

Комп'ютерне верстання *В. В. Савінкова*

Макет обкладинки *І. М. Дончик*

Формат 60 x 84/16. Ум. друк. арк. 2,11. Наклад 50 пр. Зам № 214/2021.

Видавець і виготовлювач

Харківський національний університет імені В. Н. Каразіна,

61022, м. Харків, майдан Свободи, 4.

Свідоцтво суб'єкта видавничої справи ДК № 3367 від 13.01.2009

Видавництво ХНУ імені В. Н. Каразіна

Тел. 705-24-32

Зміст

Вступ.....	4
Становлення проблеми факторизації цілих чисел	5
Інформація з використовуваних компонентів бібліотеки NT L.....	7
Опис використовуваних класів	7
Базові арифметичні оператори.....	7
Опис використовуваних процедур	7
Прості числа	9
Закон розподілу простих чисел.....	9
Імовірнісні тести на простоту	10
Прості алгоритми факторизації	11
Метод пробних поділів	11
Складність алгоритму	12
Методи прискорення алгоритму	13
Використання паралельних обчислень	14
Метод часткового перебору	14
Метод Ферма.....	16
Приклад № 1	16
Приклад № 2	17
Складність алгоритму	17
Метод решета числового поля.....	17
Решето Ератосфена і критерії простоти	18
Метод квадратичного решета	18
Метод Померанца	19
Базовий алгоритм решета числового поля.....	20
CADO-NFS: реалізація алгоритму решета числового поля	20
Установка GMP	21
Установка CADO-NFS.....	22
Установка для Ubuntu 20.04	22
Установка для Ubuntu 18.04	23
Запуск факторизації на одній машині	23
Приклад факторизації RSA-чисел	25
Завдання для самостійної роботи	28
1. Факторизація 70-бітних чисел спеціального виду ($n = p \cdot q, p \ll q$).....	28
2. Факторизація 70-бітних чисел спеціального виду ($n = p \cdot q, p \approx q$)	29
3. Факторизація 300-бітних чисел *	31
Оформлення звіту	35
Перелік джерел посилання.....	36