

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

ПРОГРАМНЕ СЕРЕДОВИЩЕ ДЛЯ РОБОТИ З ДОВГОЮ АРИФМЕТИКОЮ

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

Харків – 2021

Рецензенти:

О. В. Лемешко – доктор технічних наук, професор, завідувач кафедри інфо-комунікаційної 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)*

П 78

Програмне середовище для роботи з довгою арифметикою : методичні рекомендації до лабораторної роботи з 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. – 32 с.

Програмне середовище для роботи з довгою арифметикою розроблено для студентів факультету комп'ютерних наук за спеціальністю «Кібербезпека». У методичних рекомендаціях до лабораторної роботи з дисципліни «Теорія чисел, груп, полів, кілець» вивчаються принципи реалізації складних обчислень над числами дуже великої довжини. Зокрема, в рекомендаціях спершу коротко розглядаються різні види програмного забезпечення та спеціальних бібліотек для роботи з великими числами, а потім вирішуються конкретні практичні завдання з використанням безкоштовно постачуваного програмного забезпечення.

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

ПРОГРАМНЕ СЕРЕДОВИЩЕ ДЛЯ РОБОТИ З ДОВГОЮ АРИФМЕТИКОЮ

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

Коректор *А. І. Самсонова*

Комп'ютерне верстання *Н. Є. Пруднік*

Макет обкладинки *І. М. Дончик*

Формат 60x84/16. Ум. друк. арк. 1,6. Наклад 50 пр. Зам № 212/2021.

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.....	5
ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ДЛЯ РОБОТИ З ДОВГОЮ АРИФМЕТИКОЮ.....	7
GMP	7
NTL	7
CLN.....	7
Magma.....	8
PARI / GP.....	8
GNU Octave	9
Maple.....	9
MATLAB	9
SageMath.....	10
Sage.....	10
MPIR	10
ПІДГОТОВКА.....	11
Віртуальна машина VMware.....	11
Операційна система Ubuntu.....	12
Додатки «Термінал».....	13
Гарячі клавіші	14
Крос-компіляція для Ubuntu та підсистеми Windows для Linux.....	16
Оновлення	16
Установка оточення для розробки на C ++ для Ubuntu.....	17
Установка make.....	17
Установка компілятора C++	17
Установка m4	17
Установка NTL для UNIX.....	18
Установка GMP для UNIX.....	18
Завантаження та збирання GMP	18
Установка NTL для UNIX.....	22
Створення і запуск першої програми	25
ДОВІДНИК ІЗ КОМАНД ЗА UBUNTU.....	26
Створення папок.....	27
Файлові команди	28
Установка поточної директорії.....	28
Видалення файла/каталогу.....	28

Копіювання, створення, перейменування файла/каталогу	28
Перегляд файла	29
Використання пакетного менеджера Apt.....	29
Дисковий простір.....	29
Виставлення/зміна повноважень на файли.....	30
Виконання команд із необмеженими привілеями.....	31
ЛІТЕРАТУРА.....	32