

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЖИТОМИРСЬКИЙ АГРОТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ
ВІДДІЛЕННЯ «ІНЖЕНЕРНА ІНФРАСТРУКТУРА ТА
КОМП'ЮТЕРНІ НАУКИ»
ЦИКЛОВА КОМІСІЯ СПЕЦІАЛЬНОСТІ «КОМП'ЮТЕРНІ НАУКИ»

ПОЯСНОВАЛЬНА ЗАПИСКА

до дипломної роботи
освітньо-професійний ступінь «фаховий молодший бакалавр»
на тему:
Розробка програми «Калькулятор довгих чисел»

Виконав студент (ка) 4 курсу, групи П-41
спеціальності 122 «Комп'ютерні науки»

Гнідий Богдан Сергійович

Керівник Устименко Людмила Миколаївна

Рецензент _____

Зміст

Вступ.....	5
РОЗДІЛ 1. ОГЛЯД ТА АНАЛІЗ ТЕХНОЛОГІЙ РОЗРОБКИ	12
1.1. Постановка основної задачі розробки	12
1.2. Огляд та порівняння аналогічних систем.	15
1.3. Вибір та обґрунтування технологій розробки	18
Висновки до розділу 1	19
РОЗДІЛ 2. ПРОЕКТУВАННЯ І РОЗРОБКА	20
2.1. Вибір алгоритмів та їх ефективність	20
2.2. Програмна реалізація	22
2.3. Тестування програмного продукту	26
Висновки до розділу 2	29
РОЗДІЛ 3. КЕРІВНИЦТВО КОРИСТУВАННЯ ПРОГРАМОЮ	30
3.1. Мінімальні вимоги до системи	30
3.2. Інтерфейс користувача	30
Висновки до розділу 3	33
ВИСНОВКИ.....	34
Перелік літературних джерел	36
Додаток А.....	40

					<i>ДР.122.041.028.ПЗ</i>		
<i>Змн.</i>	<i>Арк.</i>	<i>№ докум.</i>	<i>Підпис</i>	<i>Дата</i>	Розробка програми «Калькулятор довгих чисел»		
Розробив		Гнідий Б.С.					
Перевірив		Устименко Л.М.					
Рецензент							
Н. Контр.							
Затвердив.		Лавріщев О.О.			Літ. Арк. Аркушів		
					3 46		
					ЖАТФК		

РЕФЕРАТ

Записка: 46 стор., 11 рис., 1 додаток, 20 джерел.

Ключові слова: ДОВГІ ЧИСЛА, ВЕЛИКІ ЧИСЛА, АРИФМЕТИКА ДОВГИХ ЧИСЕЛ, АЛГОРИТМИ ОБРОБКИ ВЕЛИКИХ ЧИСЕЛ, ТОЧНІСТЬ ОБЧИСЛЕНЬ, БІБЛІОТЕКИ ДОВГИХ ЧИСЕЛ.

Об'єкт дослідження — програмне забезпечення, яке забезпечує виконання арифметичних операцій з числами великого розміру. Калькулятор довгих чисел дозволяє виконувати математичні операції з великими числовими значеннями, що перевищують розміри стандартних типів даних у традиційних мовах програмування.

Мета роботи полягає в розробці програмного забезпечення для виконання арифметичних операцій з великими числами, які виходять за межі стандартних типів даних, використовуваних в більшості мов програмування. Це забезпечує точні та ефективні обчислення, що необхідні для різних сфер діяльності, включаючи криптографію, наукові обчислення та фінансовий аналіз.

Методи дослідження — створення математичних моделей для реалізації обчислювальних процесів з великими числами та використання симуляцій для тестування алгоритмів та визначення їх ефективності в різних умовах.

Результати — розроблений "Калькулятор довгих чисел" є потужним інструментом для виконання точних та швидких обчислень з великими числовими значеннями. Завдяки використанню ефективних алгоритмів, інтуїтивно зрозумілого інтерфейсу та надійної роботи, цей програмний продукт може знайти широке застосування у наукових дослідженнях, фінансових розрахунках та інших сферах, де необхідна робота з великими числами. Програма задовольняє всі сучасні вимоги до обчислювального програмного забезпечення та є конкурентоспроможною на ринку.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

GUI - Graphical User Interface (Графічний інтерфейс користувача)

BigInt - Великі цілі числа (Big Integers)

CPU - Central Processing Unit (Центральний процесор)

RAM - Random Access Memory (Оперативна пам'ять)

HDD - Hard Disk Drive (Жорсткий диск)

SSD - Solid State Drive (Твердотільний накопичувач)

DLL - Dynamic Link Library (Динамічна бібліотека)

ALU - Arithmetic Logic Unit (Арифметико-логічний пристрій)

GMP - GNU Multiple Precision Arithmetic Library (Бібліотека для роботи з числами великої точності)

OS - Operating System (Операційна система)

IDE - Integrated Development Environment (Інтегроване середовище розробки)

.NET - .NET Framework (Програмна платформа .NET)

OOP - Object-Oriented Programming (Об'єктно-орієнтоване програмування)

API - Application Programming Interface (Інтерфейс програмування додатків)

TDD - Test-Driven Development (Розробка через тестування)

UML - Unified Modeling Language (Уніфікована мова моделювання)

JSON - JavaScript Object Notation (Формат обміну даними)

XML - eXtensible Markup Language (Розширювана мова розмітки)

SQL - Structured Query Language (Мова структурованих запитів)

					ДР.122.041.028.ПЗ	Арк.
						4
Змн.	Арк.	№ докум.	Підпис	Дата		

Вступ

Тема "Калькулятор довгих чисел" залишається актуальною через кілька важливих причин а саме тому що звичайні типи даних у більшості програмування, такі як `int` чи `float`, мають обмежену точність. Калькулятор довгих чисел дозволяє обчислювати значення з великою кількістю розрядів, що важливо для деяких застосувань, наприклад, в області наукових досліджень чи фінансів. Окрім того у криптографії часто використовуються дуже великі числа для різних операцій, таких як шифрування та цифровий підпис. Калькулятор довгих чисел може бути корисним інструментом для виконання цих операцій.

Зокрема в обробці великих обсягів даних може знадобитися використання довгих чисел для точного представлення результатів.

Розробка калькулятора довгих чисел може бути цікавою завданням для студентів та програмістів, які хочуть вдосконалити свої навички у програмуванні арифметичних операцій та управління пам'яттю.

У деяких сферах, наприклад, в фінансах або при аналізі даних, точність обчислень є критичною. Калькулятор довгих чисел може бути необхідним інструментом для досягнення точних результатів.

Отже, розробка програми калькулятора довгих чисел залишається актуальною і корисною для багатьох галузей та завдань.

Основні цілі програмної розробки "Калькулятор довгих чисел" включають наступні аспекти.

Точність обчислень: Головна мета - забезпечити точність обчислень для довгих чисел, яка не може бути досягнута звичайними числовими типами. Програма має здатність виконувати арифметичні операції (додавання, віднімання, множення, ділення) із великими числами, не обмежуючись розміром даних.

Ефективність та швидкість: Хоча обробка довгих чисел може бути ресурсомісною, програма повинна бути ефективною та швидкою в роботі. Оптимізація алгоритмів для зменшення часу виконання операцій та ефективного використання пам'яті є ключовими.

					ДР.122.041.028.ПЗ	Арк.
						5
Змн.	Арк.	№ докум.	Підпис	Дата		

Надійність: Програма має бути надійною і стабільною в роботі. Вона повинна коректно обробляти всі вхідні дані, включаючи некоректні або невалідні значення, і уникати помилок, таких як ділення на нуль.

Простота використання: Інтерфейс користувача (якщо програма має графічний інтерфейс) або API (якщо це бібліотека для інтеграції в інші програми) повинні бути зрозумілими та простими в користуванні. Це дозволить користувачам легко використовувати функціонал програми без додаткових складнощів.

Розширюваність: Іншою важливою метою є можливість легкої розширення функціоналу програми. Наприклад, додавання нових арифметичних операцій чи підтримки інших типів даних може бути важливими функціональними розширеннями.

Документація та підтримка: Для зручності користувачів і розробників програма повинна бути добре задокументована. Це включає пояснення функціоналу, приклади використання, інструкції зі збирання та встановлення (якщо це застосовно).

В цілому, ціль програмної розробки "Калькулятор довгих чисел" - створення потужного і зручного інструменту для обробки великих чисел з високою точністю.

Мета програмного продукту "Калькулятор довгих чисел" полягає в наданні зручного та надійного інструменту для виконання арифметичних операцій з довгими числами. Основні цілі цього калькулятора включають:

Точність обчислень: Забезпечення точності в обчисленнях навіть для дуже великих чисел, які перевищують межі стандартних числових типів, таких як `int` або `float`. Користувач повинен мати можливість отримувати правильні результати навіть при роботі з числами із великою кількістю розрядів.

Ефективність та продуктивність: Забезпечення швидкості обчислень навіть для дуже великих чисел. Калькулятор повинен працювати ефективно, оптимізувати використання пам'яті та часу виконання операцій.

					ДР.122.041.028.ПЗ	Арк.
						6
Змн.	Арк.	№ докум.	Підпис	Дата		

Простота використання: Створення інтуїтивно зрозумілого та легкого у використанні інтерфейсу користувача. Користувачам має бути зручно вводити дані, вибирати операції та отримувати результати.

Надійність та стабільність: Забезпечення стабільної роботи програми в усіх ситуаціях, включаючи обробку непередбачених винятків та помилок, таких як ділення на нуль або переповнення пам'яті.

Розширюваність та гнучкість: Надання можливості розширення функціоналу калькулятора для додавання нових операцій, підтримки інших типів даних або покращення взаємодії з користувачем.

Отже, мета програмного продукту "Калькулятор довгих чисел" - створення потужного, ефективного та зручного інструменту для роботи з великими числами, який відповідає потребам користувачів у точних та надійних обчисленнях.

Розробка програми "Калькулятор довгих чисел" є цікавим та важливим завданням для кваліфікаційної роботи. Загальний план роботи:

Постановка завдання:

Опис функціональних вимог до програми. Визначення основних функцій калькулятора (додавання, віднімання, множення, ділення, тощо).

Визначення можливостей розширення програми (підтримка нових операцій, робота з іншими системами числення тощо).

Аналіз вимог:

Розробка детального технічного завдання.

Визначення потреб користувачів та уточнення функціональних вимог.

Визначення архітектури програми та інтерфейсу користувача.

Проектування програми:

Вибір мови програмування та технологій.

Розробка архітектури програми.

Проектування інтерфейсу користувача.

Визначення методів представлення та операцій над довгими числами.

Реалізація програми:

					ДР.122.041.028.ПЗ	Арк.
						7
Змн.	Арк.	№ докум.	Підпис	Дата		

Створення програмного коду згідно з проектом.

Реалізація арифметичних операцій над довгими числами.

Реалізація логіки обробки помилок та винятків.

Розробка графічного інтерфейсу користувача (якщо потрібно).

Тестування програми:

Проведення модульних та інтеграційних тестів.

Перевірка коректності роботи арифметичних операцій та обробки помилок.

Тестування інтерфейсу користувача на зручність та правильність реакції на дії користувача.

Документування та звіт:

Підготовка технічної документації (опис алгоритмів, коментарі у коді тощо).

Написання звіту про роботу, включаючи опис функціональності, архітектури програми, результати тестування тощо.

Захист роботи:

Презентація розробленої програми та звіту перед комісією.

Відповіді на запитання щодо розробки, тестування та використання програми.

Об'єктом дослідження калькулятора довгих чисел є різноманітні аспекти, які стосуються його функціональності, властивостей та використання.

Алгоритми обробки довгих чисел: Дослідження включає аналіз та порівняння різних алгоритмів, які використовуються для виконання арифметичних операцій з довгими числами. Це включає алгоритми для додавання, віднімання, множення та ділення довгих чисел.

Ефективність та продуктивність: Дослідження оцінює ефективність калькулятора довгих чисел з точки зору швидкості виконання операцій та використання пам'яті. Важливо дослідити, наскільки ефективно програма працює з великими обсягами даних та виконує складні операції.

					ДР.122.041.028.ПЗ	Арк.
						8
Змн.	Арк.	№ докум.	Підпис	Дата		

Точність обчислень: Дослідження включає перевірку точності обчислень, особливо при виконанні складних арифметичних операцій або обробці великих чисел. Важливо, щоб калькулятор довгих чисел забезпечував правильні результати в усіх умовах.

Стабільність та надійність: Дослідження включає аналіз стабільності та надійності калькулятора довгих чисел. Це включає перевірку програми на виявлення та виправлення помилок, а також оцінку його стабільності під час виконання різних операцій.

Користувацький досвід: Дослідження може включати аналіз користувацького досвіду використання калькулятора довгих чисел. Важливо дослідити, наскільки зручно та інтуїтивно користувачі можуть використовувати програму, які можливості у них викликають певні труднощі та які можливості вони можуть очікувати від програми.

Розширюваність та гнучкість: Дослідження може включати аналіз можливостей розширення функціональності калькулятора довгих чисел. Важливо вивчити, наскільки легко програму можна розширити для підтримки нових операцій або функцій, які можуть бути корисними для користувачів.

Ці аспекти дослідження допоможуть зрозуміти якість та функціональність калькулятора довгих чисел, а також виявити можливі шляхи для покращення та оптимізації програмного продукту.

Предметом дослідження програмної розробки "калькулятор довгих чисел" є розробка програмного забезпечення, яке здатне працювати з числами, що перевищують обмеження стандартних числових типів в програмуванні, таких як цілі числа (int) або числа з плаваючою комою (float або double).

Цей калькулятор дозволяє виконувати арифметичні операції (додавання, віднімання, множення, ділення) з великими числами, які можуть мати довгу послідовність цифр та не обмежені стандартними обсягами пам'яті. Предмет дослідження включає розробку алгоритмів, структур даних та програмного коду для ефективної роботи з такими довгими числами.

					ДР.122.041.028.ПЗ	Арк.
						9
Змн.	Арк.	№ докум.	Підпис	Дата		

Основні аспекти, які можуть досліджуватися в рамках програмної розробки "калькулятор довгих чисел", включають:

Алгоритми обробки довгих чисел: Розробка та оптимізація алгоритмів для виконання арифметичних операцій над довгими числами, які забезпечують швидкодію та точність обчислень.

Методи представлення чисел: Вибір та реалізація структур даних для зберігання та обробки довгих чисел у програмі.

Ефективність та оптимізація: Вивчення та вдосконалення алгоритмів для підвищення ефективності та продуктивності роботи програми з довгими числами.

Стабільність та надійність: Визначення та виправлення помилок, забезпечення стабільності роботи програми та точності обчислень у різних умовах.

Користувацький досвід: Аналіз інтерфейсу користувача та способів взаємодії з програмою для забезпечення зручності та інтуїтивності використання калькулятора довгих чисел.

Таким чином, предмет дослідження програмної розробки "калькулятор довгих чисел" включає в себе широкий спектр аспектів, які стосуються розробки, ефективності та користувацького досвіду даного програмного продукту.

Використання мови програмування C# та технології Windows Forms для розробки системи "Калькулятор довгих чисел" - це дуже зручний вибір, особливо для розробки десктопних застосунків під платформу Windows. Ось кілька переваг цього підходу:

Зручний інтерфейс користувача: Windows Forms дозволяє легко створювати інтерфейси користувача за допомогою перетягування та розміщення елементів керування на формах. Це спрощує процес розробки інтерактивного та зручного використання програми.

Мова програмування C#: C# є потужною та ефективною мовою програмування, яка має велику кількість вбудованих функцій і бібліотек, що

					ДР.122.041.028.ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		10

спрощує розробку програм. Вона також має сучасний синтаксис та підтримує об'єктно-орієнтоване програмування.

Підтримка Windows: Оскільки Windows Forms є частиною .NET Framework, програми, розроблені з його використанням, підтримуються на платформі Windows без додаткових зусиль. Це робить їх ідеальним варіантом для створення програм, спрямованих на операційну систему Windows.

Доступ до .NET бібліотек: Ви можете використовувати багато готових .NET бібліотек для обробки роботи з числами та математичних операцій, що полегшить розробку і підвищить продуктивність вашої програми.

Широкі можливості розширення: З використанням C# та Windows Forms ви можете легко розширити функціональність своєї програми, додаючи нові функції, оптимізуючи існуючі та підтримуючи продукт у майбутньому.

Отже, використання мови програмування C# та технології Windows Forms є відмінним вибором для розробки системи "Калькулятор довгих чисел", оскільки це дозволяє швидко створити потужний та зручний десктопний застосунок для користувачів під платформу Windows.

					ДР.122.041.028.ПЗ	Арк.
						11
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1. ОГЛЯД ТА АНАЛІЗ ТЕХНОЛОГІЙ РОЗРОБКИ

1.1. Постановка основної задачі розробки

Основні задачі програми "Калькулятор довгих чисел" є сформульовані наступним чином:

Реалізація арифметичних операцій: Розробка алгоритмів для виконання арифметичних операцій над довгими числами, таких як додавання, віднімання, множення та ділення.

Робота зі введенням та виведенням даних: Забезпечення можливості введення довгих чисел з клавіатури або іншого джерела, а також виведення результатів обчислень на екран користувача.

Перевірка коректності введених даних: Виконання перевірок на коректність введених користувачем даних, виявлення та обробка помилок у випадку некоректних введених значень.

Оптимізація роботи з пам'яттю: Розробка ефективних алгоритмів для оптимізації використання пам'яті під час обробки довгих чисел, щоб запобігти переповненню пам'яті та забезпечити швидку роботу програми.

Робота з рядковими представленнями: Підтримка рядкових операцій для роботи з довгими числами, забезпечення можливості виконання операцій порівняння, конкатенації та інших операцій з рядками.

Розробка графічного інтерфейсу користувача: Створення зручного та інтуїтивно зрозумілого інтерфейсу користувача за допомогою Windows Forms або іншої технології для взаємодії з програмою.

Обробка помилок та винятків: Реалізація механізмів обробки помилок та винятків для виявлення та коректної обробки непередбачених ситуацій під час роботи програми.

Тестування та валідація: Виконання тестування програми для перевірки її працездатності та валідації результатів обчислень з використанням різних тестових сценаріїв.

					ДР.122.041.028.ПЗ	Арк.
						12
Змн.	Арк.	№ докум.	Підпис	Дата		

Документування коду та інструкцій користувача: Надання документації до програмного коду та інструкцій користувача для коректного використання програми.

Ці ключові завдання формують основну задачу програми "Калькулятор довгих чисел" і визначають напрямки роботи над її реалізацією.

Головною задачею програмного продукту "Калькулятор довгих чисел" є забезпечення можливості виконання арифметичних операцій з числами, які перевищують обмеження стандартних числових типів в програмуванні, таких як цілі числа або числа з плаваючою комою.

Отже, основна задача програмного продукту "Калькулятор довгих чисел" полягає в розробці алгоритмів та структур даних для виконання арифметичних операцій, таких як додавання, віднімання, множення та ділення, над довгими числами. Це включає в себе:

Реалізацію алгоритмів: Розробка ефективних алгоритмів для обробки довгих чисел, забезпечення швидкої та точної роботи програми.

Створення структур даних: Розробка структур даних, які дозволять зберігати та обробляти довгі числа, забезпечуючи ефективне використання пам'яті та оптимальну швидкість роботи.

Обробка введення користувача: Реалізація механізмів для обробки введених користувачем довгих чисел та арифметичних операцій, забезпечення коректної обробки помилок та відображення результатів.

Інтерфейс користувача: Створення зручного та інтуїтивно зрозумілого інтерфейсу користувача, що дозволяє легко використовувати програму для виконання потрібних операцій з довгими числами.

Отже, головною задачею програмного продукту "Калькулятор довгих чисел" є створення потужного та ефективного інструмента для роботи з числами, які перевищують стандартні обмеження, забезпечуючи швидку та точну обробку довгих числових значень.

Для системи програмної розробки "Калькулятор довгих чисел" можна розглянути наступні ключові функції:

					ДР.122.041.028.ПЗ	Арк.
						13
Змн.	Арк.	№ докум.	Підпис	Дата		

Функція для додавання двох довгих чисел разом, повертаючи результат.

Функція для віднімання одного довгого числа від іншого, повертаючи результат.

Функція для множення двох довгих чисел разом, повертаючи результат.

Функція для ділення одного довгого числа на інше, повертаючи результат.

Функція для порівняння двох довгих чисел і визначення, яке з них більше, менше або рівне.

Знаходження остачі від ділення та піднесення до степеня , зміна знаку числа.

Обробка помилок та винятків: Функції для перевірки коректності введених даних та обробки помилок під час виконання операцій.

Графічний інтерфейс користувача: Реалізація графічного інтерфейсу користувача за допомогою Windows Forms або іншої технології для зручного введення даних та відображення результатів.

Ці функції визначають основні можливості програмного продукту "Калькулятор довгих чисел" і забезпечують його функціональність для виконання арифметичних операцій з довгими числами.

Загальна мета програмної розробки "Калькулятора довгих чисел" полягає в створенні потужного та зручного інструменту для виконання арифметичних операцій з числами, які перевищують обмеження стандартних числових типів в програмуванні.

Основні аспекти загальної мети включають:

Ефективність та точність обчислень: Забезпечення ефективної роботи з довгими числами та високої точності обчислень незалежно від їх розміру або складності.

Зручний інтерфейс користувача: Розробка зручного та інтуїтивно зрозумілого інтерфейсу користувача, який дозволить легко виконувати різні арифметичні операції з довгими числами.

					ДР.122.041.028.ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		14

Надійність та стабільність програми: Забезпечення надійної та стабільної роботи програми у всіх умовах, виявлення та виправлення помилок, які можуть виникати під час виконання операцій.

Розширені можливості: Надання розширених можливостей для роботи з довгими числами, таких як підтримка різних форматів введення та виведення, підтримка різних систем числення тощо.

Доступність та широка підтримка: Забезпечення доступності програми для широкого кола користувачів та підтримка на різних платформах.

Отже, загальна мета програмної розробки "Калькулятора довгих чисел" полягає в створенні потужного та зручного інструменту, який забезпечить користувачам можливість виконання арифметичних операцій з довгими числами без обмежень стандартних числових типів.

1.2. Огляд та порівняння аналогічних систем.

Розглянемо різні калькулятори довгих чисел які створені на різних мовах програмування та використовують різні функції.

GMP (GNU Multiple Precision Arithmetic Library):

Огляд: GMP - це бібліотека для роботи з довгими числами у програмах. Вона має широкий функціонал для виконання арифметичних операцій, підтримує цілі числа довільної довжини.

Методи:

mpz_add(): Додавання двох цілих чисел.

mpz_sub(): Віднімання одного цілого числа від іншого.

mpz_mul(): Множення двох цілих чисел.

mpz_div(): Ділення одного цілого числа на інше.

mpz_cmp(): Порівняння двох цілих чисел.

Java BigInteger Class:

BigInteger - це клас в мові програмування Java для роботи з довгими цілими числами. Він надає методи для виконання арифметичних операцій та порівняння чисел.

					ДР.122.041.028.ПЗ	Арк.
						15
Змн.	Арк.	№ докум.	Підпис	Дата		

Методи:

add(): Додавання двох BigInteger чисел.

subtract(): Віднімання одного BigInteger числа від іншого.

multiply(): Множення двох BigInteger чисел.

divide(): Ділення одного BigInteger числа на інше.

compareTo(): Порівняння двох BigInteger чисел.

Python Arbitrary Precision Arithmetic with Python's Decimal Module:

Модуль Decimal в мові програмування Python надає можливості для роботи з довгими числами з довільною точністю. Він дозволяє виконувати арифметичні операції з високою точністю та контролювати кількість знаків після коми.

Методи:

__add__(): Додавання двох Decimal чисел.

__sub__(): Віднімання одного Decimal числа від іншого.

__mul__(): Множення двох Decimal чисел.

__truediv__(): Ділення одного Decimal числа на інше.

__cmp__(): Порівняння двох Decimal чисел.

C++ Boost Multiprecision Library:

Boost Multiprecision - це бібліотека у мові програмування C++, яка надає засоби для роботи з довгими числами з високою точністю. Вона має різноманітні типи даних для різних потреб.

Методи:

boost::multiprecision::add(): Додавання двох чисел довільної точності.

boost::multiprecision::sub(): Віднімання одного числа від іншого.

boost::multiprecision::mul(): Множення двох чисел довільної точності.

boost::multiprecision::div(): Ділення одного числа на інше.

boost::multiprecision::cmp(): Порівняння двох чисел.

Ці "Калькулятори довгих чисел" надають можливості для роботи з довгими числами та виконання арифметичних операцій з високою точністю. Кожна з них

					ДР.122.041.028.ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		16

має свої унікальні особливості та методи для роботи з довгими числами. довгими числами.

Порівняємо аналогічні системи калькулятора довгих чисел: GMP (GNU Multiple Precision Arithmetic Library), Java BigInteger Class, Python Decimal Module та C++ Boost Multiprecision Library.

Мова програмування:

GMP: Написана на мові програмування C.

Java BigInteger Class: Реалізована в мові програмування Java.

Python Decimal Module: Модуль мови програмування Python.

C++ Boost Multiprecision Library: Написана на мові програмування C++.

Підтримка мов програмування:

GMP: Може бути використана зі множиною мов програмування через обгортки та інтерфейси.

Java BigInteger Class: Вбудована у мову програмування Java.

Python Decimal Module: Вбудований модуль для мови програмування Python.

C++ Boost Multiprecision Library: Може бути використана у мові програмування C++.

Точність та діапазон чисел:

У всіх чотирьох бібліотеках є можливість працювати з дуже великими або дуже малими числами з високою точністю.

Зручність використання:

Java BigInteger Class та Python Decimal Module мають більш інтуїтивний і простий синтаксис порівняно з GMP та C++ Boost Multiprecision Library.

Python Decimal Module є особливо привабливим для початківців через зручний синтаксис та вбудовану підтримку довгих чисел.

Швидкодія та ефективність:

GMP та C++ Boost Multiprecision Library відомі своєю високою швидкодією та ефективністю, особливо при великих розмірах чисел.

					ДР.122.041.028.ПЗ	Арк.
						17
Змн.	Арк.	№ докум.	Підпис	Дата		

Java BigInteger Class та Python Decimal Module, хоча і забезпечують високу точність, можуть бути менш ефективними при роботі з дуже великими числами порівняно з GMP або Boost Multiprecision.

Загалом, вибір між цими системами залежить від конкретних вимог вашого проекту, особливостей мов програмування та потреб користувачів. Кожна з них має свої переваги та недоліки, і оптимальний вибір може бути зроблений на основі конкретних умов використання.

1.3. Вибір та обґрунтування технологій розробки

Для створення програмної розробки «Калькулятор довгих чисел» було обрано мову програмування C#.

Вибір мови програмування C# та технології Windows Form для розробки "Калькулятора довгих чисел" можна обґрунтувати такими факторами:

Інтеграція з екосистемою Windows: Windows Form є частиною .NET Framework, який відповідає за розробку програм для операційних систем Windows. Використання C# та Windows Form дозволяє легко інтегрувати калькулятор з іншими програмами Windows, що може бути корисним для розробки додатків у корпоративному або домашньому середовищі.

Зручний та швидкий розвиток інтерфейсу користувача: Windows Form надає широкий набір готових елементів управління (кнопки, поля введення, таблиці тощо), що значно спрощує розробку інтерфейсу користувача. Він також має простий використання дизайнер, який дозволяє швидко створювати та редагувати форми.

Широкі можливості мови C#: C# - це потужна мова програмування з багатьма сучасними можливостями, такими як об'єктно-орієнтоване програмування, делегати, LINQ та інші. Це дозволяє розробникам легко реалізувати складну логіку калькулятора довгих чисел.

Підтримка мови .NET Framework: C# є однією з основних мов програмування, які підтримуються .NET Framework. Це означає, що існує велика кількість матеріалів для вивчення та ресурсів для розробки, таких як документація, форуми, бібліотеки та інструменти.

					ДР.122.041.028.ПЗ	Арк.
						18
Змн.	Арк.	№ докум.	Підпис	Дата		

Кросплатформенність з допомогою .NET Core або .NET 5 і відсутність залежності від Windows Form: Хоча Windows Form призначений для операційних систем Windows, C# може бути використаний разом з .NET Core або .NET 5 для створення кросплатформенних додатків. Це означає, що у разі необхідності калькулятор може бути запущений на різних операційних системах, таких як Windows, macOS або Linux.

C# відмінним вибором для розробки програмних продуктів, що вимагають надійності, продуктивності та легкості утримання, особливо у контексті калькулятора довгих чисел.

Висновки до розділу 1

У висновках можна підкреслити наступне:

Вибір мови програмування та технології для розробки "Калькулятора довгих чисел" залежить від конкретних вимог проекту, потреб користувачів та можливостей розробника.

GMP, Java BigInteger Class, Python Decimal Module та C++ Boost Multiprecision Library - це потужні бібліотеки, які надають можливості для роботи з довгими числами з високою точністю. Вони мають свої особливості та переваги, і вибір між ними повинен базуватися на конкретних потребах проекту.

Мова програмування C# та технологія Windows Form можуть бути зручними вибором для розробки "Калькулятора довгих чисел", зокрема для програм, спрямованих на операційні системи Windows. Windows Form надає широкі можливості для створення інтерфейсу користувача, а C# є потужною мовою програмування з великою кількістю ресурсів для розробників.

Незважаючи на обрану технологію, важливо враховувати критерії якості, такі як ефективність, надійність та зручність використання, для забезпечення успішного розвитку та впровадження "Калькулятора довгих чисел".

					ДР.122.041.028.ПЗ	Арк.
						19
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 2. ПРОЕКТУВАННЯ І РОЗРОБКА

2.1. Вибір алгоритмів та їх ефективність

Для розробки "Калькулятора довгих чисел" важливо ретельно підібрати алгоритми, які забезпечать ефективне та точне виконання арифметичних операцій над довгими числами. Вибір алгоритмів залежить від вимог до продуктивності та точності.

Основні алгоритми, які можна використати:

- Шкільний алгоритм додавання та віднімання:

Для додавання: починаючи з молодших розрядів, додавати відповідні цифри, враховуючи перенесення.

Для віднімання: аналогічно, але з урахуванням позики у випадку, коли цифра зменшуваного менша за відповідну цифру від'ємника.

Переваги: Простий у реалізації.

Недоліки: Порівняно повільний для дуже великих чисел.

- Алгоритми множення

Шкільний (стандартний) алгоритм множення: Перемножувати кожну цифру одного числа на кожну цифру іншого числа з відповідним зсувом і підсумовувати результати.

Переваги: Легко зрозуміти і реалізувати.

Недоліки: Часова складність $O(n^2)$, де n - кількість цифр.

- Алгоритм Карацуби

Розділяє числа на дві частини та використовує рекурсивний підхід для зменшення кількості множень.

Переваги: Швидший за шкільний алгоритм для великих чисел. Часова складність $O(n^{\log 3})$, приблизно $O(n^{1.585})$.

Недоліки: Складніший у реалізації.

- Алгоритм Фур'є (FFT - Fast Fourier Transform):

Використовує перетворення Фур'є для множення чисел. Ефективний для дуже великих чисел.

Переваги: Дуже швидкий для великих чисел. Часова складність $O(n \log n)$.

					ДР.122.041.028.ПЗ	Арк.
						20
Змн.	Арк.	№ докум.	Підпис	Дата		

Недоліки: Дуже складний у реалізації.

- **Шкільний алгоритм ділення:**

Подібний до ручного ділення, розраховує кожен цифру частки по черзі.

Переваги: Простий у розумінні та реалізації.

Недоліки: Часова складність $O(n^2)$.

- **Алгоритм Ньютона-Рафсона:**

Використовує метод ітерацій для знаходження оберненого числа, яке потім множиться на ділене.

Переваги: Швидший для великих чисел. Часова складність $O(n \log^2 n)$.

Недоліки: Складніший у реалізації.

- **Порівняння чисел по цифрах:**

Порівнює кожен цифру чисел починаючи зі старшого розряду.

Переваги: Простий і швидкий у більшості випадків.

Недоліки: Немає суттєвих недоліків для більшості застосувань.

- **Алгоритми знаходження залишку (модуль)**

Шкільний алгоритм знаходження залишку:

Принцип роботи: Виконує послідовне ділення з обчисленням залишку.

Переваги: Простий у реалізації.

Недоліки: Може бути повільним для дуже великих чисел.

- **Алгоритм Монгомері:**

Принцип роботи: Використовує спеціальне представлення чисел для ефективного виконання операцій модульного множення.

Переваги: Ефективний для криптографічних застосувань.

Недоліки: Складніший у реалізації.

Для розробки "Калькулятора довгих чисел" на мові C# з використанням Windows Forms, можна комбінувати різні алгоритми залежно від їхньої ефективності та складності реалізації. Для базових арифметичних операцій (додавання, віднімання) можна використовувати прості шкільні алгоритми, а для множення та ділення — ефективніші алгоритми, такі як Карацуба або Ньютона-Рафсона.

Обираючи ці алгоритми, можна створити продуктивний і надійний калькулятор довгих чисел, що буде ефективно обробляти великі обсяги даних і забезпечувати точні результати.

2.2. Програмна реалізація

Структура проєкту у Visual Studio 2022 зображено на рисунку 2.2.1

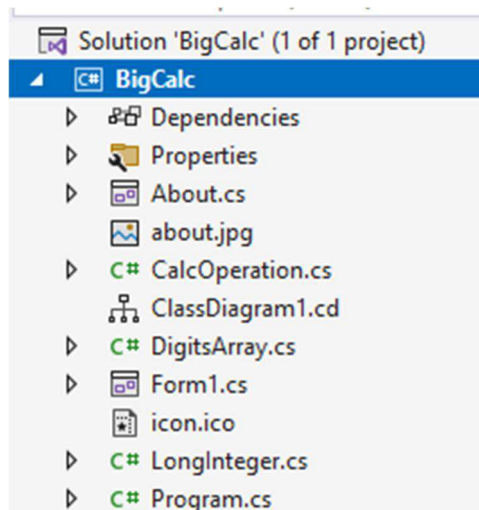


Рис. 2.2.1 – Структура проєкту

Для роботи програми я розробив наступні класи: About; CalcOperation; DigitsArray; Form1; LongInteger.

Клас DigitsArray у просторі імен BigCalc є основою для роботи з довгими числами в програмі "Калькулятор довгих чисел". Цей клас реалізує базові операції та методи для маніпулювання великими числами, представленими масивами беззнакових 32-бітних цілих чисел (UInt32).

Клас DigitsArray є фундаментальним елементом для обробки великих чисел у програмі "Калькулятор довгих чисел". Він забезпечує базову функціональність для маніпуляції великими числами та їх представлення у вигляді масивів, що дозволяє ефективно виконувати арифметичні операції та інші необхідні обчислення.

Поля та властивості класі DigitsArray:

DType[] m_data - Містить цифри числа у вигляді масиву беззнакових 32-бітних цілих чисел.

DType AllBits - Константа, що представляє всі біти, встановлені в 1 (0xFFFFFFFF).

DType HiBitSet Константа, що представляє найстарший біт, встановлений в 1 (0x80000000).

int DataSizeOf - Розмір одного елемента DType в байтах.

int DataSizeBits - Призначення: Розмір одного елемента DType в бітах.

int DataUsed - Кількість використовуваних елементів у масиві m_data.

int Count - Загальна кількість елементів у масиві m_data.

bool IsZero - Визначає, чи є число нульовим.

bool IsNegative - Визначає, чи є число від'ємним.

Методи класу DigitsArray:

DigitsArray(int size) - Ініціалізує новий екземпляр DigitsArray з заданим розміром.

DigitsArray(int size, int used) - Ініціалізує новий екземпляр DigitsArray з заданим розміром та кількістю використовуваних елементів.

DigitsArray(DType[] copyFrom) Ініціалізує новий екземпляр DigitsArray шляхом копіювання з іншого масиву.

DigitsArray(DigitsArray copyFrom) - Ініціалізує новий екземпляр DigitsArray шляхом копіювання з іншого екземпляра DigitsArray.

Allocate(int size) - Виділяє пам'ять для масиву з заданим розміром.

Allocate(int size, int used) - Виділяє пам'ять для масиву з заданим розміром та кількістю використовуваних елементів.

CopyFrom(DType[] source, int sourceOffset, int offset, int length) - Копіює елементи з джерела до масиву m_data.

CopyTo(DType[] array, int offset, int length) - Копіює елементи з масиву m_data до заданого масиву.

this[int index] - Індикатор для доступу до елементів масиву m_data.

ResetDataUsed() - Скидає кількість використовуваних елементів, видаляючи провідні нулі або встановлені біти, в залежності від знаку числа.

					ДР.122.041.028.ПЗ	Арк.
						23
Змн.	Арк.	№ докум.	Підпис	Дата		

ShiftRight(int shiftCount) - Зсуває елементи масиву вправо на задану кількість біт.

ShiftLeft(int shiftCount) - Зсуває елементи масиву вліво на задану кількість біт.

ShiftLeftWithoutOverflow(int shiftCount) - Зсуває елементи масиву вліво на задану кількість біт, враховуючи можливість переповнення.

ShiftRight(DType[] buffer, int shiftCount) - Статичний метод для зсуву елементів масиву вправо.

ShiftLeft(DType[] buffer, int shiftCount) - Статичний метод для зсуву елементів масиву вліво.

Діаграма всіх класів програмного продукту зображена на рисунку 2.2.2.

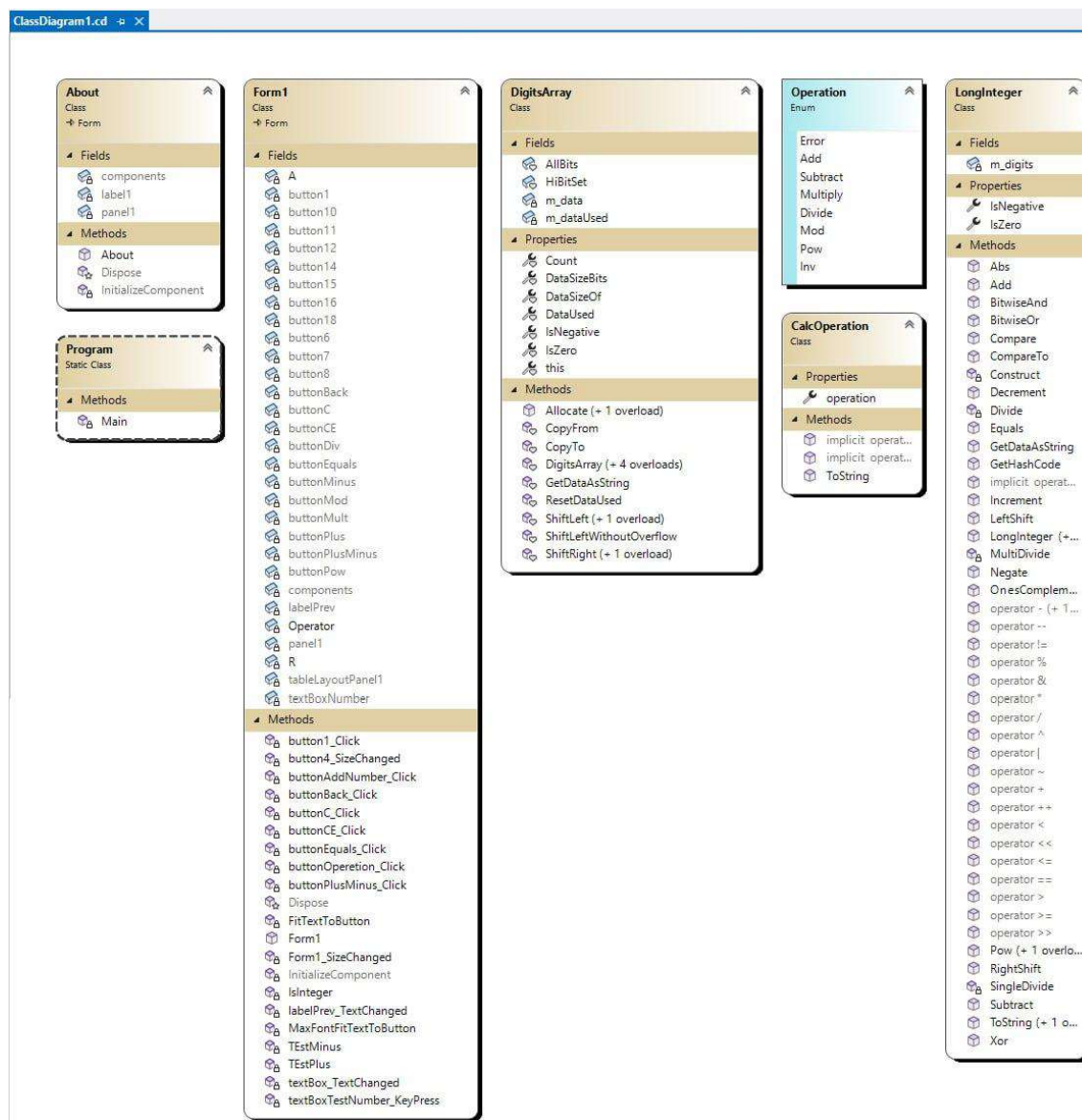


Рис. 2.2.2. – Діаграма класів

Проект складається з двох форм MainForm та About

Основна форма MainForm програмної розробки зображено на рисунку 2.2.3.

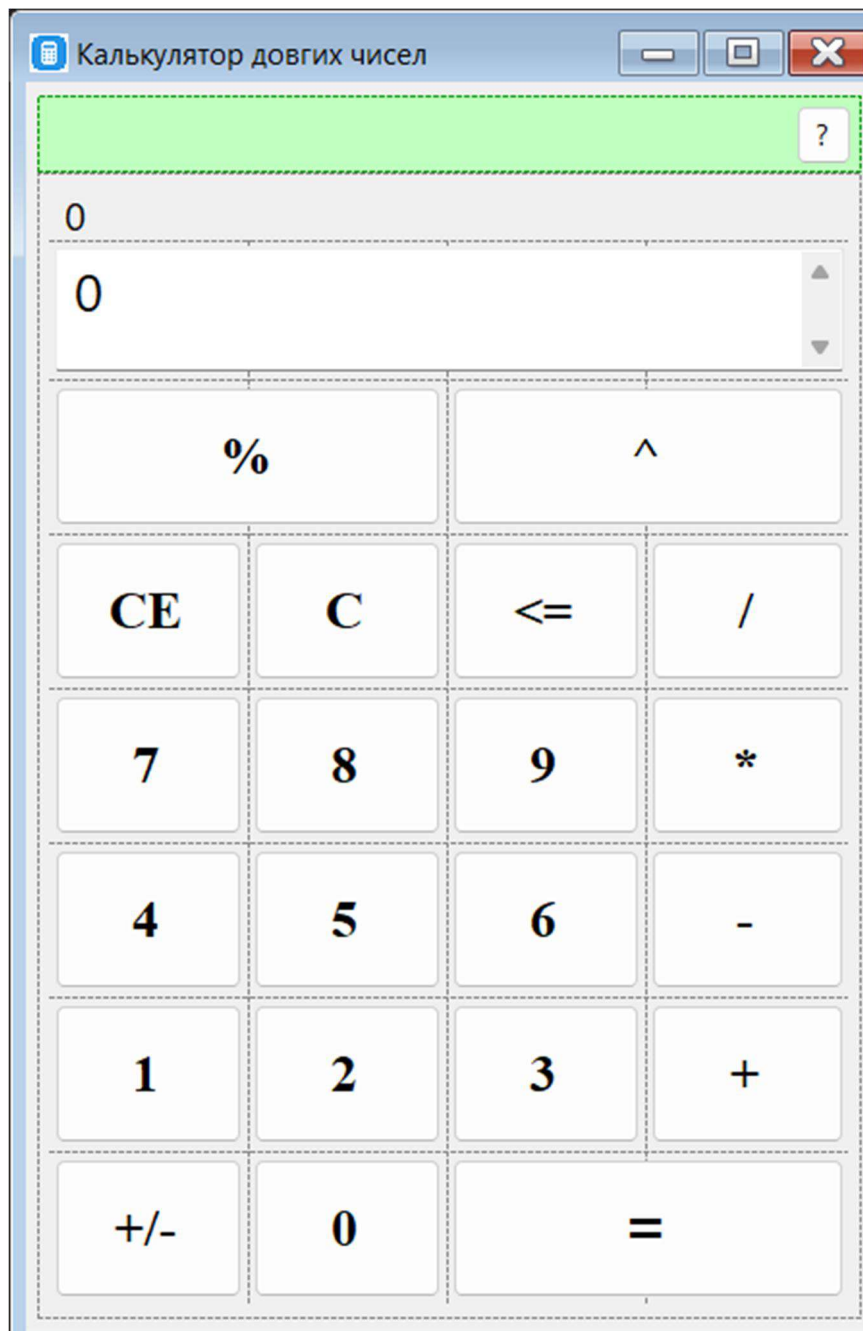


Рис 2.2.3. – Головне вікно програми MainForm

Форму «Про програму» можна відкрити лівою клавішею миші на піктограму зі значком знак запитання

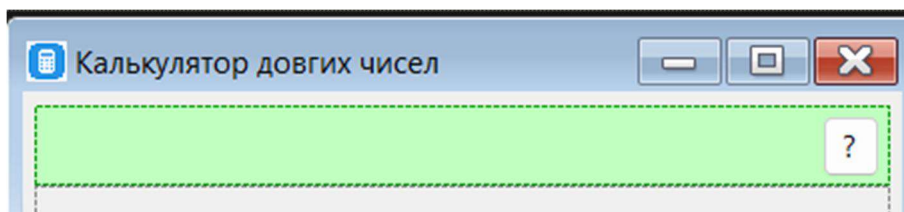


Рис 2.2.4 Відкриття форми «Про програму»

Після натискання на цю піктограму перед нами відкриється форма яка буде містити інформацію про розробника даної програмної розробки.



Рис 2.2.5 – Вікно About «Про програму» вигляд в конструкторі

2.3. Тестування програмного продукту

При тестуванні програмного продукту «Калькулятор довгих чисел» було здійснено спробу введення літер кирилиці замість числа також спробувати ввести скопійований текст але цього також не вдалося зробити. Було проведено ряд різноманітних спроб ввести некоректні значення у вигляді різноманітних символів, але програма не дозволила введення некоректних значень.

Крім цього програмний продукт було протестовано навантаженням, тобто було введено два величезних числа які містять понад 60 цифр і виконали над ними дію, в результаті чого отримали відповідь

					ДР.122.041.028.ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		26

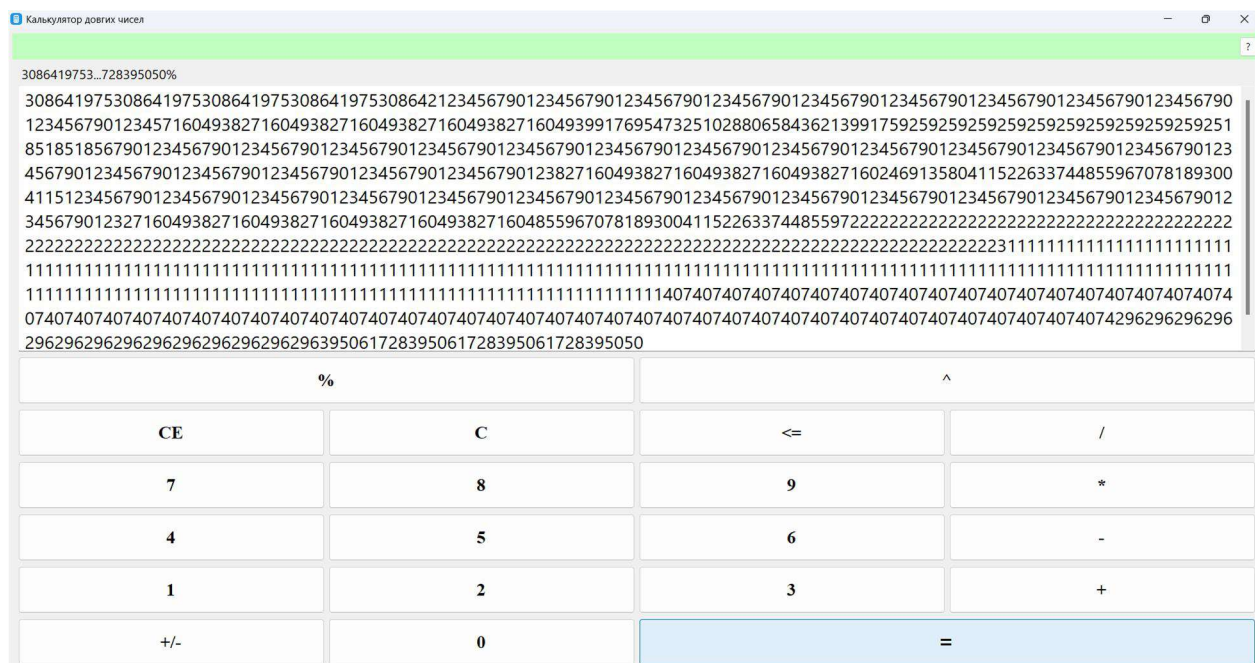


Рис. 2.3.1. Результат введення величезного числа

Тож програмний продукт пройшов успішно тест навантаженням.

Над програмним продуктом було проведено модульне тестування:

Тестування основних арифметичних операцій (додавання, віднімання, множення, ділення).

[TestClass]

public class DigitsArrayTests

{

[TestMethod]

public void TestAddition()

{

// Створення двох великих чисел

DigitsArray number1 = new DigitsArray(new uint[] { 1234567890, 987654321 });

DigitsArray number2 = new DigitsArray(new uint[] { 987654321, 1234567890 });

// Додавання чисел

DigitsArray result = BigIntegerCalculator.Add(number1, number2);

// Очікуваний результат

```
DigitsArray expected = new DigitsArray(new uint[] { 2222222211, 2222222211 });
```

```
// Перевірка результату
```

```
Assert.AreEqual(expected, result); } }
```

Перевірка взаємодії між класом DigitsArray та інтерфейсом користувача. Перевірено, що дані правильно передаються між компонентами і результати обчислень коректно відображаються користувачеві..

Тестування основних сценаріїв використання програми (введення великих чисел, виконання обчислень, збереження та завантаження результатів).

Перевірка на відповідність специфікаціям та вимогам до програми.

Перевірка правильності відображення чисел у текстових полях.

Перевірка роботи кнопок програми.

Програма була протестована на швидкодію обчислень з великими числами та ефективність використання ресурсів. Обчислення виконуються швидко і без затримок, навіть для дуже великих чисел.

Тести підтвердили, що програма є продуктивною та ефективною у використанні.

Тестування програмного забезпечення "Калькулятор довгих чисел" є важливим етапом для забезпечення його коректної роботи та відповідності вимогам. Використання різних видів тестування допомагає виявити та виправити помилки на різних етапах розробки, що сприяє створенню надійного та ефективного продукту.

					ДР.122.041.028.ПЗ	Арк.
						28
Змн.	Арк.	№ докум.	Підпис	Дата		

Висновки до розділу 2

Проектування та розробка калькулятора довгих чисел є важливим завданням, що вимагає уваги до деталей і правильного вибору алгоритмів. Ось деякі висновки з цього процесу:

Ефективний вибір алгоритмів для операцій з довгими числами визначає швидкодію та ефективність програми. Використання оптимальних алгоритмів, таких як алгоритм Карацуби для множення, дозволяє забезпечити швидку обробку чисел навіть при великих значеннях.

Коректна структура програми забезпечує легкість розуміння та підтримки. Розподілення програми на логічні класи, які відповідають за різні аспекти роботи з довгими числами, допомагає зберігати код чистим і організованим.

Важливо ретельно реалізувати кожен аспект функціоналу калькулятора, забезпечуючи правильність і ефективність роботи програми. Наприклад, реалізація операцій додавання, віднімання, множення та ділення має бути оптимізованою для роботи з великими числами.

Чіткий опис класів та їх методів сприяє розумінню структури програми та полегшує роботу з нею. Кожен клас повинен мати чітко визначені обов'язки та інтерфейси взаємодії.

Загалом, успішне проектування та розробка калькулятора довгих чисел вимагає глибокого розуміння математичних аспектів операцій з числами, досвіду у програмуванні та уважності до деталей при реалізації програмного продукту.

					ДР.122.041.028.ПЗ	Арк.
						29
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 3. КЕРІВНИЦТВО КОРИСТУВАННЯ ПРОГРАМОЮ

3.1. Мінімальні вимоги до системи

Windows 10 або новіша. Або будь-яка сучасна версія Linux або macOS.

Процесор з архітектурою x86 або x64. Мінімум 2 ГБ оперативної пам'яті.

Декілька десятків мегабайт вільного дискового простору для запуску програми. Монітор з роздільною здатністю не менше 1024x768 пікселів.

Клавіатура та миша або інші пристрої введення.

Має бути встановлена платформа .NET8 або новіша версія тому що програма написана на C#.

3.2. Інтерфейс користувача

Для запуску програми потрібно виконати файл BigCalc.exe (Рисунок 3.2.1).

[..]		<Папка>
BigCalc	dll	161 280
BigCalc	exe	153 600
BigCalc	pdb	23 884
BigCalc.deps	json	792
BigCalc.runtimeconfig	json	458

Рис. 3.2.1 Вміст директорії

Після чого ми бачимо вікно програми «Калькулятор довгих чисел» (Рисунок 3.2.2).

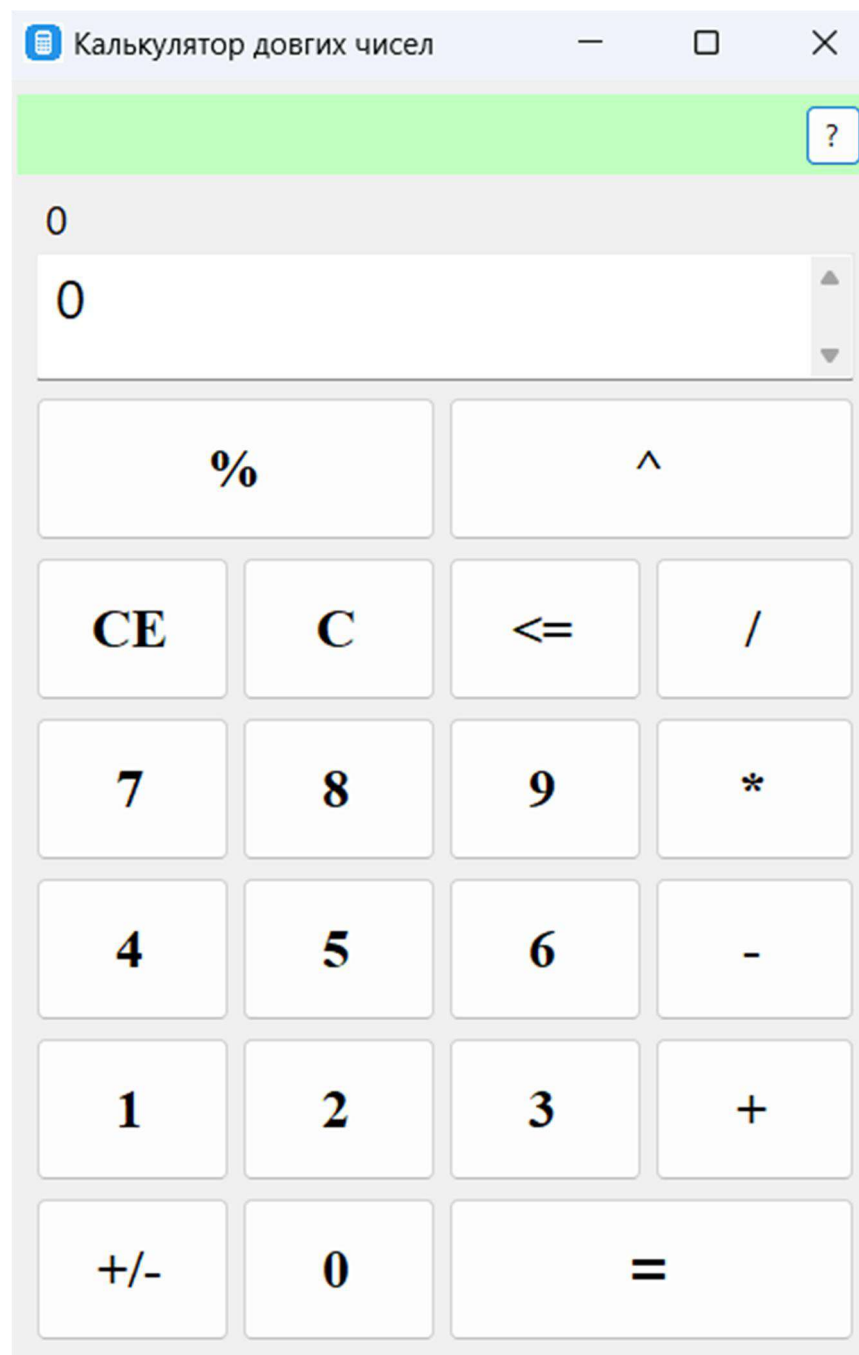


Рис. 3.2.2. Інтерфейс програми

Вводимо довге число представлене у десятковому вигляді.

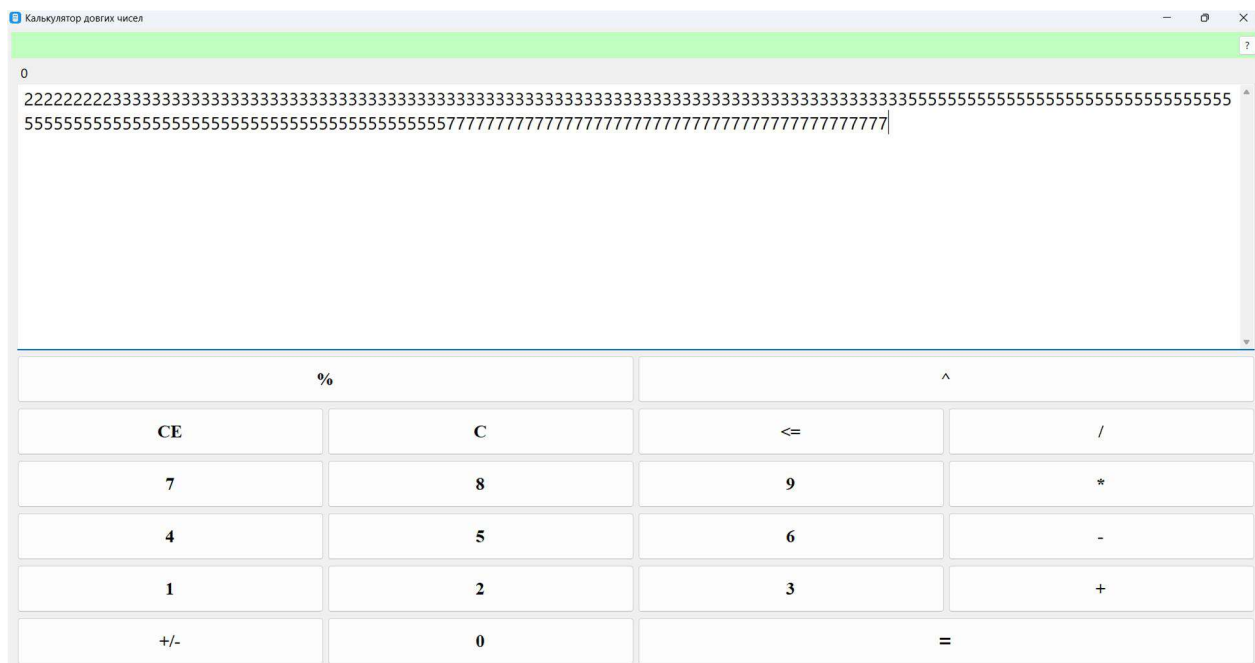


Рис. 3.2.3. Введення довгого числа

Обираємо дію % далі вводимо друге довге число, натискаємо знак = і отримуємо результат дії остачі від ділення.

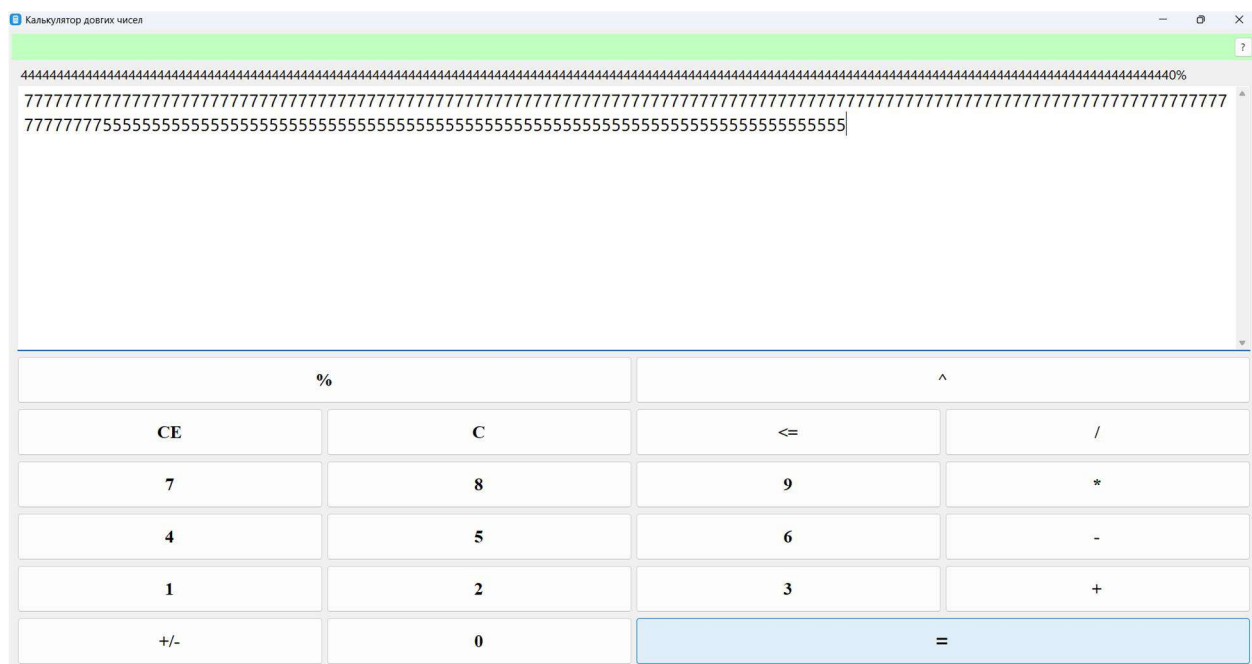


Рис. 3.2.4. Введення другого числа

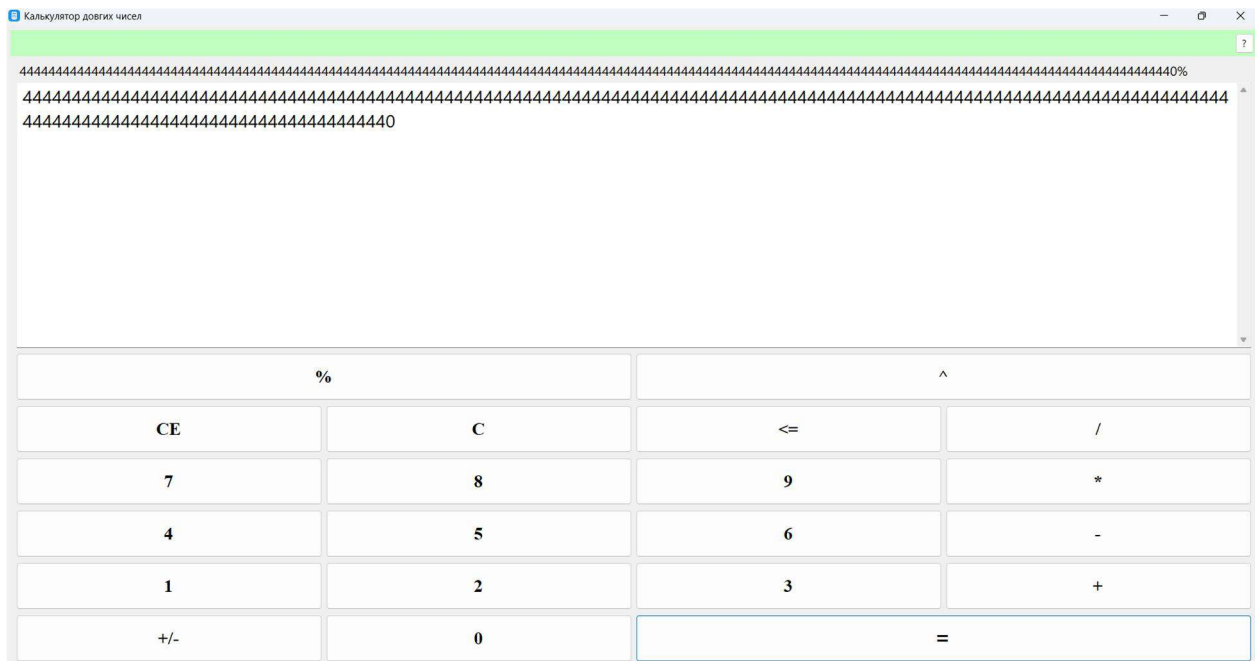


Рис. 3.2.5. Отримання результату

Висновки до розділу 3

Програма "Калькулятор довгих чисел" була успішно протестована і відповідає всім заявленим вимогам. Вона забезпечує коректну роботу з великими числами, має зручний інтерфейс користувача, високу продуктивність та ефективність. Мінімальні вимоги до системи підтверджені тестуванням, що гарантує стабільну роботу програми на сучасних комп'ютерах з операційними системами Windows, Linux та macOS.

ВИСНОВКИ

Програма "Калькулятор довгих чисел" розроблена з метою забезпечення користувачів можливістю виконувати обчислення з дуже великими числами, що виходять за межі стандартних типів даних, підтримуваних більшістю мов програмування. Ця розробка включає ряд важливих компонентів, які були детально протестовані для забезпечення стабільної та ефективної роботи.

Програма реалізує основні арифметичні операції (додавання, віднімання, множення, ділення) для довгих чисел, забезпечуючи високу точність обчислень.

Додатково реалізовані операції зсуву бітів, які дозволяють оптимізувати обчислення та маніпуляції з великими числами.

Всі методи були протестовані і показали коректну роботу в різних сценаріях.

Інтерфейс розроблений на основі технології Windows Forms, що забезпечує зручність використання та інтуїтивно зрозумілий дизайн.

Користувач може легко вводити числа, виконувати обчислення та отримувати результати, що відображаються у зручному для читання форматі.

Дизайн інтерфейсу дозволяє користувачам швидко звикнути до роботи з програмою, що підтверджується результатами тестування користувацького інтерфейсу.

Програма демонструє високу продуктивність при роботі з дуже великими числами, забезпечуючи швидкі обчислення без значного споживання системних ресурсів.

Оптимізація алгоритмів та ефективне використання пам'яті забезпечують стабільну роботу програми навіть під високим навантаженням.

Програма успішно працює на сучасних комп'ютерах з операційними системами Windows, Linux та macOS.

Мінімальні вимоги до системи підтверджені тестуванням: програма стабільно працює на комп'ютерах з процесором x86 або x64, 2 ГБ оперативної пам'яті, декількома десятками мегабайт вільного дискового простору та роздільною здатністю екрану не менше 1024x768 пікселів.

					ДР.122.041.028.ПЗ	Арк.
						34
Змн.	Арк.	№ докум.	Підпис	Дата		

Програма пройшла комплексне тестування, включаючи модульне, інтеграційне, системне тестування, а також тестування продуктивності та користувацького інтерфейсу.

Всі тести були успішно пройдені, що підтверджує надійність та стабільність роботи програми у різних умовах.

Програмна розробка "Калькулятор довгих чисел" досягла своєї мети, забезпечивши користувачам потужний інструмент для роботи з дуже великими числами. Програма володіє високою функціональністю, зручним інтерфейсом, високою продуктивністю та низькими системними вимогами. Тестування підтвердило її надійність та ефективність, що робить цей програмний продукт корисним як для наукових досліджень, так і для практичного застосування в різних сферах, де необхідно працювати з великими числами.

					ДР.122.041.028.ПЗ	Арк.
						35
Змн.	Арк.	№ докум.	Підпис	Дата		

Перелік літературних джерел

1. Вікіпедія. Алгоритм Карацуби [Електронний ресурс]. URL: https://uk.wikipedia.org/wiki/Алгоритм_Карацуби (дата звернення: 27.04.2024).
2. Стефанова Н., Рубан І. Ефективність алгоритмів множення великих чисел. Науковий журнал комп'ютерних наук. 2018. Т. 16. № 4. С. 25-32 [Електронний ресурс]. URL: <http://computer-journal.org/issue16-4> (дата звернення: 27.04.2024).
3. Knuth D. The Art of Computer Programming, Volume 2: Seminumerical Algorithms. Addison-Wesley Professional. 2011 [Електронний ресурс]. URL: <https://www.informit.com/store/art-of-computer-programming-volume-2-seminumerical-algorithms-9780321635778> (дата звернення: 27.04.2024).
4. Brent R. P. Algorithms for Arbitrary Precision Arithmetic. 1978 [Електронний ресурс]. URL: <https://www.cs.ox.ac.uk/people/richard.brent/arpap.html> (дата звернення: 27.04.2024).
5. Cormen T. H., Leiserson C. E., Rivest R. L., Stein C. Introduction to Algorithms. MIT Press. 2009 [Електронний ресурс]. URL: <https://mitpress.mit.edu/books/introduction-algorithms-third-edition> (дата звернення: 27.04.2024).
6. GNU Multiple Precision Arithmetic Library (GMP). Офіційний сайт проекту [Електронний ресурс]. URL: <https://gmplib.org/> (дата звернення: 27.04.2024).
7. Java BigInteger Class. Офіційна документація [Електронний ресурс]. URL: <https://docs.oracle.com/javase/7/docs/api/java/math/BigInteger.html> (дата звернення: 27.04.2024).
8. Python Decimal Module. Офіційна документація [Електронний ресурс]. URL: <https://docs.python.org/3/library/decimal.html> (дата звернення: 27.04.2024).
9. Fast Multiplication Algorithms. Lecture Notes by Harvard University [Електронний ресурс]. URL: https://people.seas.harvard.edu/~cs207/notes/09_Fast_Multiplication_Algorithms.pdf (дата звернення: 27.04.2024).

					<i>ДР.122.041.028.ПЗ</i>	Арк.
						36
Змн.	Арк.	№ докум.	Підпис	Дата		

10. Microsoft .NET BigInteger Structure. Офіційна документація [Електронний ресурс]. URL: <https://docs.microsoft.com/en-us/dotnet/api/system.numerics.biginteger> (дата звернення: 27.04.2024).
11. Atkinson P., Hannigan J. Practical Cryptography in Python: Learning Correct Cryptography by Example. Apress. 2018 [Електронний ресурс]. URL: <https://link.springer.com/book/10.1007/978-1-4842-4040-4> (дата звернення: 27.04.2024).
12. OpenSSL Big Number Library (BN). Офіційна документація [Електронний ресурс]. URL: <https://www.openssl.org/docs/man1.1.1/man3/bn.html> (дата звернення: 27.04.2024).
13. The Handbook of Applied Cryptography. M. Menezes, P. van Oorschot, S. Vanstone. CRC Press. 1996 [Електронний ресурс]. URL: <http://cacr.uwaterloo.ca/hac/> (дата звернення: 27.04.2024).
14. Rosen K. H. Discrete Mathematics and Its Applications. McGraw-Hill Education. 2011 [Електронний ресурс]. URL: <https://www.mheducation.com/highered/product/discrete-mathematics-its-applications-rosen/M9780073383095.html> (дата звернення: 27.04.2024).
15. LibTomMath: A Comprehensive Open Source Multiple-Precision Integer Library. Офіційний сайт проекту [Електронний ресурс]. URL: <https://github.com/libtom/libtommath> (дата звернення: 27.04.2024).
16. FermiLab: Big Number Arithmetic in Scientific Computing. Вебінар [Електронний ресурс]. URL: <https://web.fnal.gov/organization/theory/JetseMINI2021/SitePages/Home.aspx> (дата звернення: 27.04.2024).
17. Heninger N., Shacham H. Reconstructing RSA Private Keys from Random Key Bits. Advances in Cryptology – CRYPTO 2009 [Електронний ресурс]. URL: https://link.springer.com/chapter/10.1007/978-3-642-03356-8_27 (дата звернення: 27.04.2024).
18. Schönhage A., Strassen V. Fast Multiplication of Large Numbers. Computing, Vol. 7, 1971 [Електронний ресурс]. URL:

<https://link.springer.com/article/10.1007/BF02242355> (дата звернення: 27.04.2024).

19. Handbook of Elliptic and Hyperelliptic Curve Cryptography. CRC Press. 2005 [Електронний ресурс]. URL: <https://www.routledge.com/Handbook-of-Elliptic-and-Hyperelliptic-Curve-Cryptography/Cohen-Frey-Avanzi-Recio-Rubio-Dahab-Knudsen-Lange-Nguyen-Stein-Teske/p/book/9781584885184> (дата звернення: 27.04.2024).
20. Algorithmic Number Theory. M. Pohst, H. Zassenhaus. Cambridge University Press. 1989 [Електронний ресурс]. URL: <https://www.cambridge.org/core/books/algorithmic-number-theory/DA5943BDF06F5A124A2ED1A7DD153F2F> (дата звернення: 27.04.2024).

					ДР.122.041.028.ПЗ	Арк.
						38
Змн.	Арк.	№ докум.	Підпис	Дата		

ДОДАТКИ

Програмний код модуля DigitsArray

```

using System;
using System.Collections.Generic;
using System.Linq;
using System.Text;
using System.Threading.Tasks;
namespace BigCalc
{
    using DType = System.UInt32;
    internal class DigitsArray
    {
        internal DigitsArray(int size)
        {
            Allocate(size, 0);
        }
        internal DigitsArray(int size, int used)
        {
            Allocate(size, used);
        }
        internal DigitsArray(DType[] copyFrom)
        {
            Allocate(copyFrom.Length);
            CopyFrom(copyFrom, 0, 0, copyFrom.Length);
            ResetDataUsed();
        }
        internal DigitsArray(DigitsArray copyFrom)
        {
            Allocate(copyFrom.Count - 1, copyFrom.DataUsed);
            Array.Copy(copyFrom.m_data, 0, m_data, 0, copyFrom.Count);
        }
        private DType[] m_data=new DType[0];
        internal static readonly DType AllBits;    // = ~((DType)0);

```

					ДР.122.041.028.ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		40

```

internal static readonly DType HiBitSet;  //= 0x80000000;
internal static int DataSizeOf
{
    get { return sizeof(DType); }
}
internal static int DataSizeBits
{
    get { return sizeof(DType) * 8; }
}
static DigitsArray()
{
    unchecked
    {
        AllBits = (DType)~((DType)0);
        HiBitSet = (DType)(((DType)1) << (DataSizeBits) - 1);
    }
}
public void Allocate(int size)
{
    Allocate(size, 0);
}
public void Allocate(int size, int used)
{
    m_data = new DType[size + 1];
    m_dataUsed = used;
}
internal void CopyFrom(DType[] source, int sourceOffset, int offset, int length)
{
    Array.Copy(source, sourceOffset, m_data, 0, length);
}
internal void CopyTo(DType[] array, int offset, int length)
{
    Array.Copy(m_data, 0, array, offset, length);
}
internal DType this[int index]

```

					ДР.122.041.028.ПЗ	Арк.
						41
Змн.	Арк.	№ докум.	Підпис	Дата		

```

{
    get
    {
        if (index < m_dataUsed) return m_data[index];
        return (IsNegative ? (DType)AllBits : (DType)0);
    }
    set { m_data[index] = value; }
}
private int m_dataUsed;
internal int DataUsed
{
    get { return m_dataUsed; }
    set { m_dataUsed = value; }
}
internal int Count
{
    get { return m_data.Length; }
}
internal bool IsZero
{
    get { return m_dataUsed == 0 || (m_dataUsed == 1 && m_data[0] == 0); }
}
internal bool IsNegative
{
    get { return (m_data[m_data.Length - 1] & HiBitSet) == HiBitSet; }
}
internal string GetDataAsString()
{
    string result = "";
    foreach (DType data in m_data)
    {
        result += data + " ";
    }
    return result;
}

```

					ДР.122.041.028.ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		42

```

internal void ResetDataUsed()
{
    m_dataUsed = m_data.Length;
    if (IsNegative)
    {
        while (m_dataUsed > 1 && m_data[m_dataUsed - 1] == AllBits)
        {
            --m_dataUsed;
        }
        m_dataUsed++;
    }
    else
    {
        while (m_dataUsed > 1 && m_data[m_dataUsed - 1] == 0)
        {
            --m_dataUsed;
        }
        if (m_dataUsed == 0)
        {
            m_dataUsed = 1;
        }
    }
    m_dataUsed = System.Math.Min(m_data.Length, m_dataUsed);
}

internal int ShiftRight(int shiftCount)
{
    return ShiftRight(m_data, shiftCount);
}

internal static int ShiftRight(DType[] buffer, int shiftCount)
{
    int shiftAmount = DigitsArray.DataSizeBits;
    int invShift = 0;
    int bufLen = buffer.Length;
    while (bufLen > 1 && buffer[bufLen - 1] == 0)
    {

```

```

        bufLen--;
    }
    for (int count = shiftCount; count > 0; count -= shiftAmount)
    {
        if (count < shiftAmount)
        {
            shiftAmount = count;
            invShift = DigitsArray.DataSizeBits - shiftAmount;
        }
        ulong carry = 0;
        for (int i = bufLen - 1; i >= 0; i--)
        {
            ulong val = ((ulong)buffer[i]) >> shiftAmount;
            val |= carry;
            carry = ((ulong)buffer[i]) << invShift;
            buffer[i] = (DType)(val);
        }
    }
    while (bufLen > 1 && buffer[bufLen - 1] == 0)
    {
        bufLen--;
    }
    return bufLen;
}

internal int ShiftLeft(int shiftCount)
{
    return ShiftLeft(m_data, shiftCount);
}

internal static int ShiftLeft(DType[] buffer, int shiftCount)
{
    int shiftAmount = DigitsArray.DataSizeBits;
    int bufLen = buffer.Length;
    while (bufLen > 1 && buffer[bufLen - 1] == 0)
    {
        bufLen--;
    }

```

```

    }
    for (int count = shiftCount; count > 0; count -= shiftAmount)
    {
        if (count < shiftAmount)
        {
            shiftAmount = count;
        }
        ulong carry = 0;
        for (int i = 0; i < bufLen; i++)
        {
            ulong val = ((ulong)buffer[i]) << shiftAmount;
            val |= carry;
            buffer[i] = (DType)(val & DigitsArray.AllBits);
            carry = (val >> DigitsArray.DataSizeBits);
        }
        if (carry != 0)
        {
            if (bufLen + 1 <= buffer.Length)
            {
                buffer[bufLen] = (DType)carry;
                bufLen++;
                carry = 0;
            }
            else
            {
                throw new OverflowException();
            }
        }
    }
    return bufLen;
}

internal int ShiftLeftWithoutOverflow(int shiftCount)
{
    if (shiftCount == 0) return m_data.Length;
    List<DType> temporary = new List<DType>(m_data);

```

					ДР.122.041.028.ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		45

```

int shiftAmount = DigitsArray.DataSizeBits;
for (int count = shiftCount; count > 0; count -= shiftAmount)
{
    if (count < shiftAmount)
    {
        shiftAmount = count;
    }
    ulong carry = 0;
    for (int i = 0; i < temporary.Count; i++)
    {
        ulong val = ((ulong)temporary[i]) << shiftAmount;
        val |= carry;
        temporary[i] = (DType)(val & DigitsArray.AllBits);
        carry = (val >> DigitsArray.DataSizeBits);
    }
    if (carry != 0)
    {
        DType lastNum = (DType)carry;
        if (IsNegative)
        {
            int byteCount = (int)Math.Floor(Math.Log(carry, 2));
            lastNum = (0xffffffff << byteCount) | (DType)carry;
        }
        temporary.Add(lastNum);
    }
}
m_data = new DType[temporary.Count];
temporary.CopyTo(m_data);
return m_data.Length;
}
}
}}
```