Лабораторна робота № 1.

**Тема: „Вибір та реалізація базових фреймворків та бібліотек”.**

**Мета роботи: «Вибір базових бібліотек/сервісів для подальшої реалізації криптосистеми».**

Завдання роботи:

Для першого типу лабораторних робіт - дослідження алгоритмів реалізації арифметичних операцій над великими (багато розрядними) числами над скінченими полями та групами з точки зору їх ефективності за часом та пам’яттю для різних програмно-апаратних середовищ.

Варіанти завдань першого типу. Дослідити бібліотеки багатослівної арифметики:

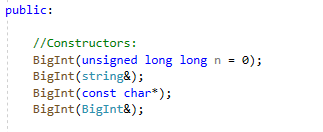
* Підгрупа 1А. Бібліотеки багаторозрядної арифметики, вбудовані в програмні платформи С++/С# (BigInteger), Java (BigInt) та Python (обрати одну з них) для процесорів із 32-розрядною архітектурою та обсягом оперативної пам’яті до 8 ГБ (робочі станції).

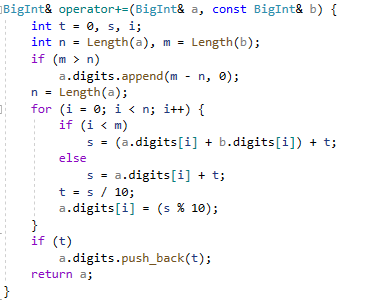
Оформлення результатів роботи. Опис функції багато розрядної арифметики обраної бібліотеки з описом алгоритму та оцінками їх складності, вхідних та вихідних даних, кодів повернення. Контрольний приклад роботи з функціями.

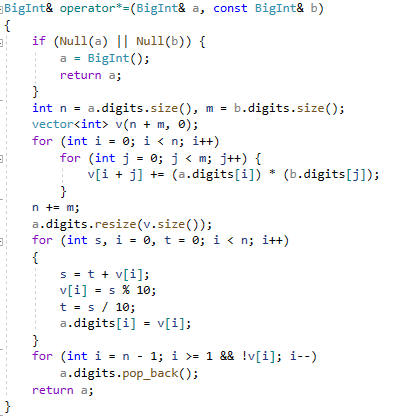
**Аналіз**

**BigInt**

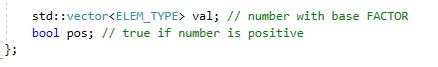
****

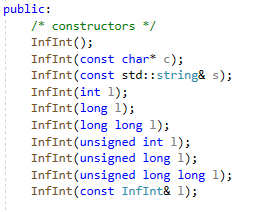
****

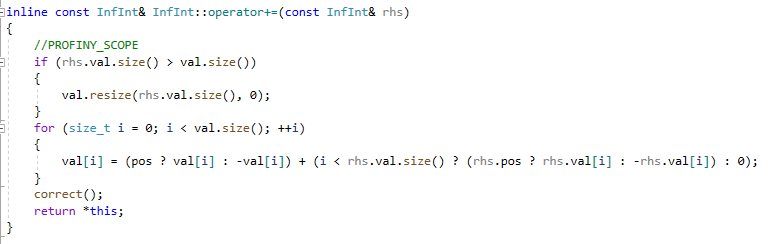
****

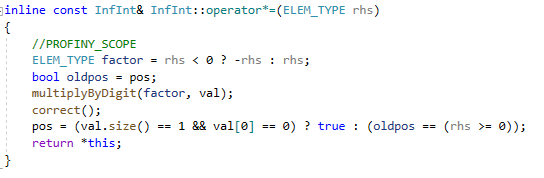
****

**InfInt**

****

****

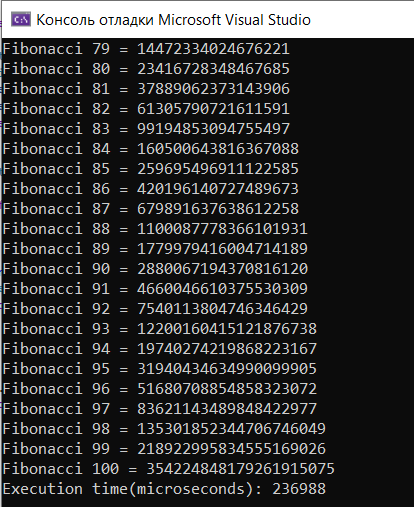
****

****

**Приклад та порівняння витрат по часу**

**Числа Фібоначі**

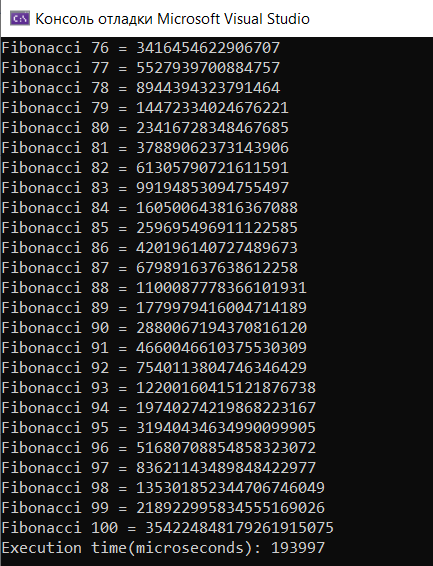
**BigInt**



AVG time for 10 runs: 205787

AVG time for 100 runs: 177707

**InfInt**

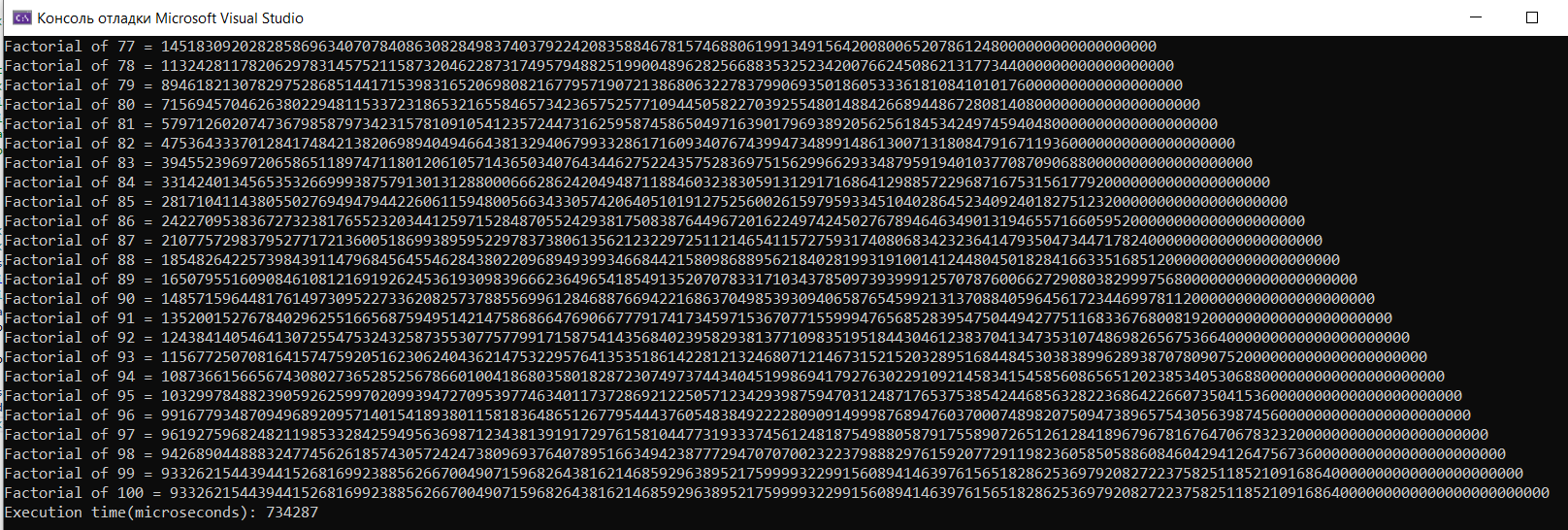


AVG time for 10 runs: 205652

AVG time for 100 runs: 172090

**Факторіал**

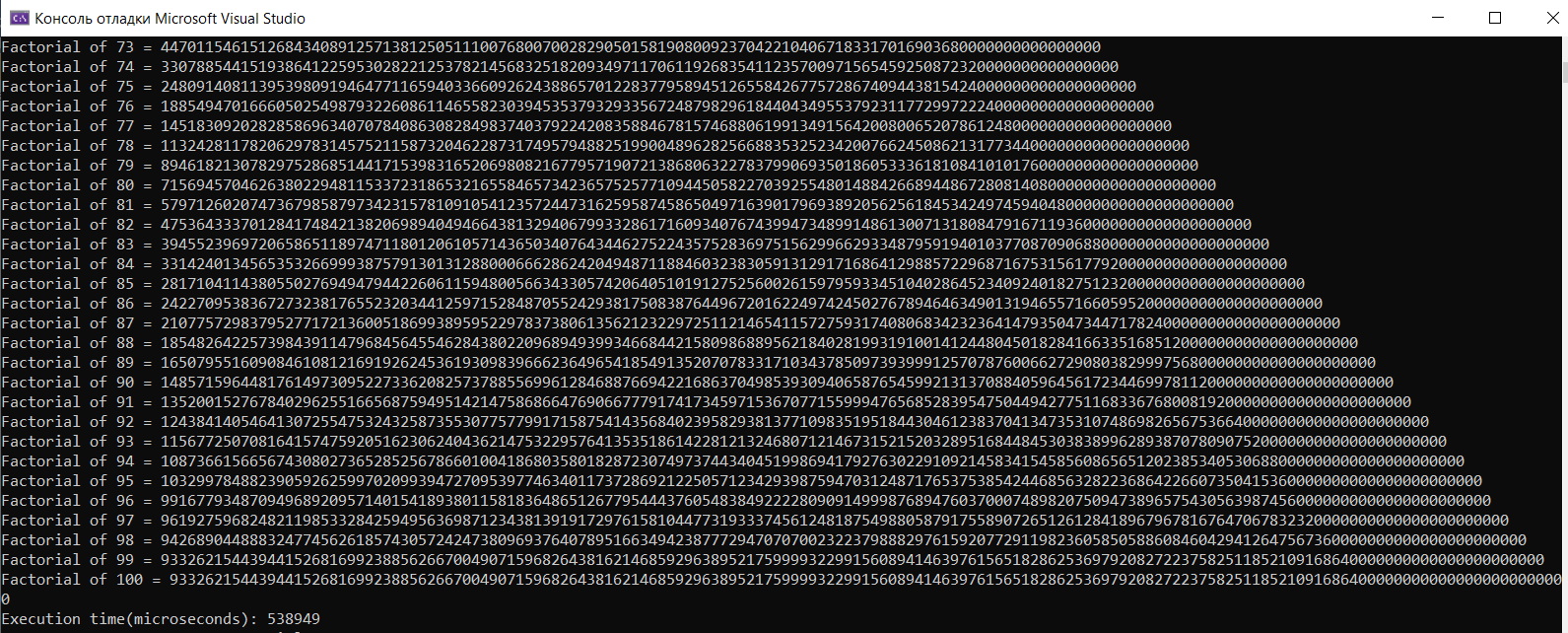
**BigInt**

****

AVG time for 10 runs: 714589

AVG time for 100 runs: 654676

**InfInt**

****

AVG time for 10 runs: 540800

AVG time for 100 runs: 455622