**СПЕЦІАЛЬНІ РОЗДІЛИ**

**ОБЧИСЛЮВАЛЬНОЇ МАТЕМАТИКИ**

**КОМП’ЮТЕРНИЙ ПРАКТИКУМ No2**

**Багаторозрядна модулярна арифметика**

**1. Мета роботи**

Отримання практичних навичок програмної реалізації багаторозрядної арифметики;

ознайомлення з прийомами ефективної реалізації критичних по часу ділянок програмного коду та методами оцінки їх ефективності.

**3. Завдання до комп’ютерного практикуму**

А) Доопрацювати бібліотеку для роботи з m-бітними цілими числами, створену на

комп’ютерному практикумі No1, додавши до неї такі операції:

1) обчислення НСД та НСК двох чисел;

2) додавання чисел за модулем;

3) віднімання чисел за модулем;

4) множення чисел та піднесення чисел до квадрату за модулем;

5) піднесення числа до багаторозрядного степеня d по модулю n .

num1 = Number(base, "CBE75E23D145C3DC78D76739B63D337CC33268E08CE4EA7319C38B7D057B1747D59010759F3B015858DC5A9D05DDBBD3EF41A368BA1CA6D8A6D967F2FED6B7033E7F56D46BEAE7C259CCE870E0879F49849C956B6B6810BE90D0C50C54DAAEF41B2B1C6E3C7B2ED35DA549A7C95FD551841EA90E4196E8272B42EA3DBA7CDCEF")

num2 = Number(base, "D0A166BEF0F8CD687A755CE64C4736E2621FE749AF3C4170354C55A2728037612CF3B134550036E2DE888E049EE782AB82AB99BA3442A3B4B8EB21C9F79778CFF4CE0C2109A02FD18163E5155146D156B92176C03BA2B87EE53BA78217529616EEA6E8432B0F736B09E30E89F3CEEAEA11FB94DACD994E1FD8A6059CC14A58B2")

mod = Number(base, "247A")

Сума двох чисел: DC1

Час виконання: 0.9380407333374023 секунд

Різниця двох чисел: 635

Час виконання: 0.8816444873809814 секунд

Добуток двох чисел: B52

Час виконання: 7.504594802856445 секунд

Степінь двох чисел: 1ED1

Час виконання: 5.595376968383789 секунд

Test completed

Завдання з НСД та НСК я виконав не повністю.Для чисел не дуже великої довжини алгоритм працює, але для таких великих чисел час роботи алгоритму склав 5 хвилин, що не є оптимальним.