## 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.

2. 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.

Код програми виконаний мовою JavaScript

Перевірка коректності:

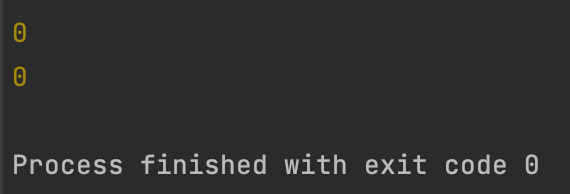
let ***first*** = hexModMul(hexModSum(***a***.hex, ***b***.hex, ***n***.hex), ***c***.hex, ***n***.hex);

let ***second*** = hexModMul(***c***.hex, hexModSum(***a***.hex, ***b***.hex, ***n***.hex), ***n***.hex);

let ***third*** = findHexFraction(hexSum(hexMul(***a***.hex, ***c***.hex), hexMul(***b***.hex, ***c***.hex)), ***n***.hex);

***console***.log(compare(***first***, ***second***));

***console***.log(compare(***second***, ***third***));



Функція compare виводить 0 коли на вхід подаються однакові значення, з чого робимо висновок що first=second=third, отже операції коректні

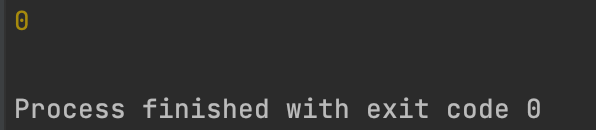
let ***result*** = hexModMul(***a***.hex,"100", ***n***.hex), ***res*** = "";

for(let i = 0; i < 100; i++){

***res*** = hexModSum(***res***, ***a***.hex, ***n***.hex);

}

***console***.log(compare(***result***,***res***));



З чого робимо висновок про коректність модулярного множення на константу



n=3^k k=256

let ***a*** = new BigNumber("e0eca40fa47eb1d99af1838e3511901f51a7056dd93fad40a69bd32ee7ffbd203cc8d6a1259daa8d36adbed57b78ddb8a3e405fb8e4d4ab0a51d16a59654335815579b95bc87231d0126e9e4cbcf375ef39a76e8b6c8f9828e73dce22faf72f74eb34237e0a13605d4c23efbcbf3a61cc710944f06a9c6b55efb9c7bcd5efb2");

let ***b*** = new BigNumber("35d511ab97c4c85188b4964af58b4c596f8ddcc7adeeb80d4fff81fed242815e55bc8375a205de07597d51d2105f2f0730f401");

let ***n*** = new BigNumber("23e3611d0fd8858bb0786431f907883b9fb3e8851e9f255e355501548c2c563ee3d3024e6c03e95a3ba8e136b594ca04cb4d56");

let ***actual*** = hexModPow(***a***.hex, ***b***.hex, ***n***.hex);

***console***.log(***actual***);



Час виконання операцій (взято середнє значення при 10 запусках)

| Операція/значення | Мінімальне | Максимальне | Середнє |
| --- | --- | --- | --- |
| Додавання (модулярне) | 20.567ms | 57.328 ms | 26.17ms |
| Віднімання (модулярне) | 24.895ms | 53.671ms | 30.7ms |
| Множення (модулярне) | 62.974ms | 99.606ms | 71.37ms |
| Піднесення до степеня | 55.357s | 56.034s | 55.67s |

// Всі вхідні змінні мають розрядність 512, включаючи степінь