

Міністерство освіти і науки України

НТУУ«Київський політехнічний інститут»

Фізико-технічний інститут

Спеціальні розділи обчислювальної

Лабораторна робота

Робота №1

**Виконав:**

Студент 3 курсу ФТІ

групи ФІ-03

Недождій М. А.

**Перевірила:**

Пекарчук Н. А.

## 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 C++, залито на GitHub

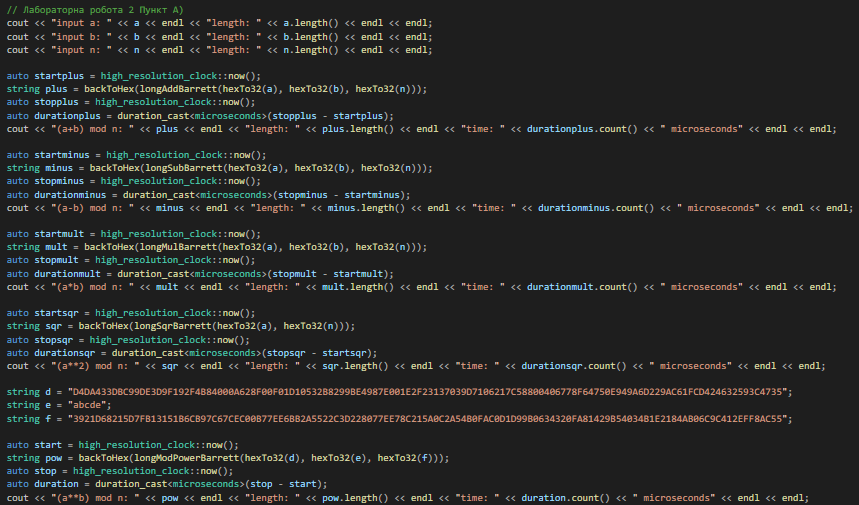
Дані на вхід для +,-,\*,\*\*2 mod n:

string a = "94EDE1A444B9738ADF06CDB40DCAFA87B25A8BECA2D2262A53D8431A119405F0CBEFB83D2AD547CCE3AE74A8EC74A313C8BED20D4349D9EFBA356FE6E8AD89E2";

string b = "5BCC0B222EE17877C9EB60FA91632BC7A6E29D80F02CD3FE16B5C2A2231B43DB2B2D12F21B293AAF49FE1165CB7A21D12D6ACEC225285544B36BABD3F8B4DD8D";

string c = "2AB3786D3A85E62EC763A05A73A7F08D21EEE3CBCAE207E40854121BFF8258F7B2B293B0D30277CDB987A6FCB5BF28B68D8E68ABA88DED37BD80A879A1BB53E3";

string n = "8E06E4DFFB37B57A66ECC52CF2D7D888C49C2794E6FB944C4183A128203932FEBEA4B6E62B2EBDAD4FF0B80DBEDC8439D31280D13E7E523596D92861F6A89E81";



Дані на вхід для a\*\*b mod n:

string d = "D4DA433DBC99DE3D9F192F4B84000A628F00F01D10532B8299BE4987E001E2F23137039D7106217C58800406778F64750E949A6D229AC61FCD424632593C4735";

string e = "abcde";

string f = "3921D68215D7FB13151B6CB97C67CEC00B77EE6BB2A5522C3D228077EE78C215A0C2A54B0FAC0D1D99B0634320FA81429B54034B1E2184AB06C9C412EFF8AC55";

Текст у консолі:

input a: 94EDE1A444B9738ADF06CDB40DCAFA87B25A8BECA2D2262A53D8431A119405F0CBEFB83D2AD547CCE3AE74A8EC74A313C8BED20D4349D9EFBA356FE6E8AD89E2

length: 128

input b: 5BCC0B222EE17877C9EB60FA91632BC7A6E29D80F02CD3FE16B5C2A2231B43DB2B2D12F21B293AAF49FE1165CB7A21D12D6ACEC225285544B36BABD3F8B4DD8D

length: 128

input n: 8E06E4DFFB37B57A66ECC52CF2D7D888C49C2794E6FB944C4183A128203932FEBEA4B6E62B2EBDAD4FF0B80DBEDC8439D31280D13E7E523596D92861F6A89E81

length: 128

(a+b) mod n: 62B307E67863368842056981AC564DC694A101D8AC0365DC290A6494147616CD387814491ACFC4CEDDBBCE00F91240AB23171FFE29F3DCFED6C7F358EAB9C8EE

length: 128

time: 261314 microseconds

(a-b) mod n: 3921D68215D7FB13151B6CB97C67CEC00B77EE6BB2A5522C3D228077EE78C215A0C2A54B0FAC0D1D99B0634320FA81429B54034B1E2184AB06C9C412EFF8AC55

length: 128

time: 280420 microseconds

(a\*b) mod n: 3FFAB6F5A2EDE763F69744D4CB856D1C3C68A17DE0777F3E33628F8EB8EBB1A51819DF1970A832C2A9C7E569805A27F321BCA9220956C407AE7A4D4EAD465649

length: 128

time: 259002 microseconds

(a\*\*2) mod n: 5878B78A1EC44E22F1277FFCE75F85596CBE3200DA3D4610F96DFE54A724499AAF2F9AE667B1535295D0D65C261622F48D7BBE0E4881AC10335B181F7DB6B33F

length: 128

time: 271099 microseconds

(a\*\*b) mod n: 173F3A6AB1A5A684AE7C33788F465689DC6791823377AB81833FF66844CCC1F506D20060873C720449BB608AF46201322F37C9986952402AF9A8315BCCB30A7

length: 127

time: 11788416 microseconds

Б) перевірки на коректність



Текст у консолі:

(a+b)\*c = c\*(a+b) mod n

(a+b)\*c = a\*c + b\*c mod n

c\*(a+b) = a\*c + b\*c mod n

n\*a = a+a+...+a mod m

time: 46914134 microseconds

a\*\*(p-1)=1 mod p

a\*\*(2\*3\*\*(k-1))=1 mod 3\*\*k

**Час виконання операцій у мікросекундах**

|  |  |  |  |
| --- | --- | --- | --- |
| Операція  Значення | Мінімальне | Середнє | Максимальне |
| Додавання | 237070 | 260811 | 304501 |
| Віднімання | 244845 | 276169 | 308254 |
| Множення | 248657 | 261351 | 271098 |
| Квадрат | 252981 | 278637 | 309563 |
| Піднесення до степеня\* | 11456957 | 11960220 | 12703730 |

\*піднесення виконувалося на числі яке довжиною 128 в hex до степеня довжиною 5 в hex за модулем довжиною 128 в hex.