Міністерство освіти і науки України
Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського"
Фізико-технічний інститут

Дисципліна “Спеціальні розділи обчислювальної математики”
Комп’ютерний практикум

Робота №2

Виконав
студент гр. ФБ-11 Подолянко Т.О.
Перевірив
Грубіян Є.О.

Київ — 2023

Робота №2. Багаторозрядна модулярна арифметика

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.

Завдання до комп'ютерного практикуму згідно з варіантом №13

А) Доопрацювати бібліотеку для роботи з m-бітними цілими числами, створену на комп’ютерному практикумі №1, 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 .

Модулярну арифметику рекомендовано реалізовувати на базі редукції Баррета, піднесення до степеня – на базі схеми Горнера. Мова програмування, семантика функцій та спосіб реалізації можуть обиратись довільним чином.

Окрім основного завдання, ви також можете виконати додаткове завдання згідно варіанту.

Хід роботи

Завдання практикуму реалізовано мовою програмування Rust. Вихідні коди розміщено у інтернет-репозиторії GitHub за посиланням: https://github.com/timofey282228/sprzom-lab1_2.git.

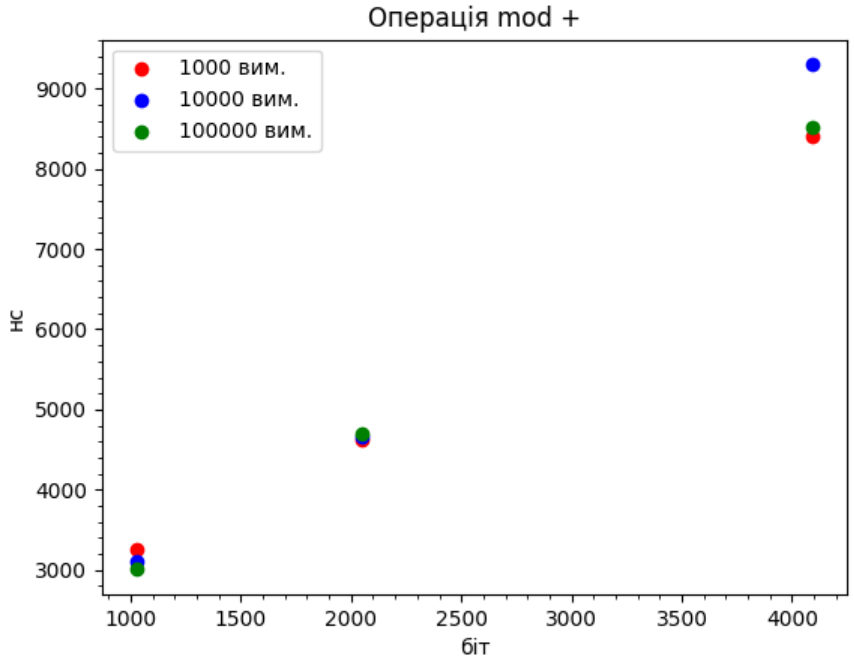
Для контролю коректності роботи алгоритмів реалізовані відповідні юніт-тести. Контрольні результати отримані за допомогою наданого онлайн-ресурсу: https://srom-check.herokuapp.com/calculate-long-arithmetic, та через порівняння із операціями на класі BigInteger у Java.

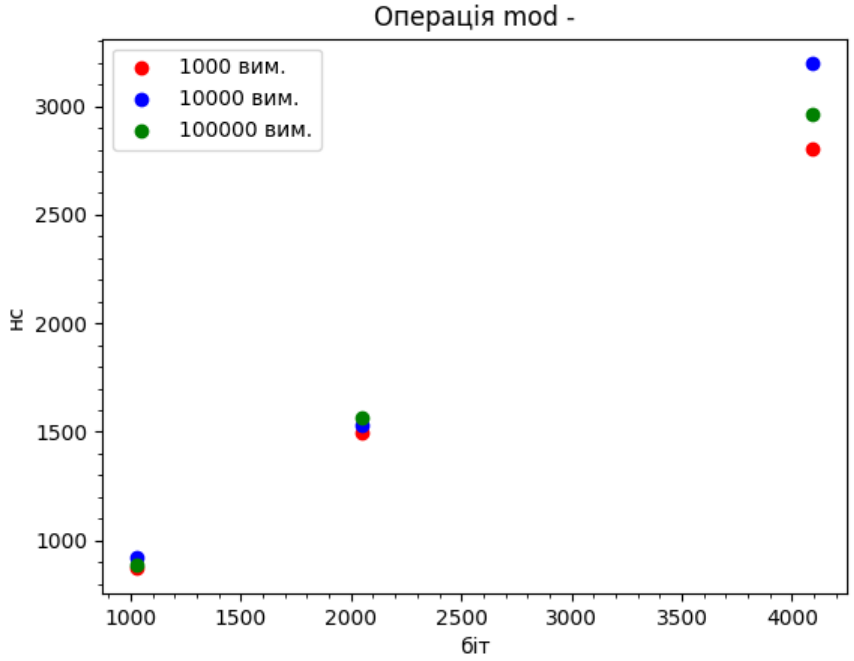
Результати виконання тестів за пунктом Б:

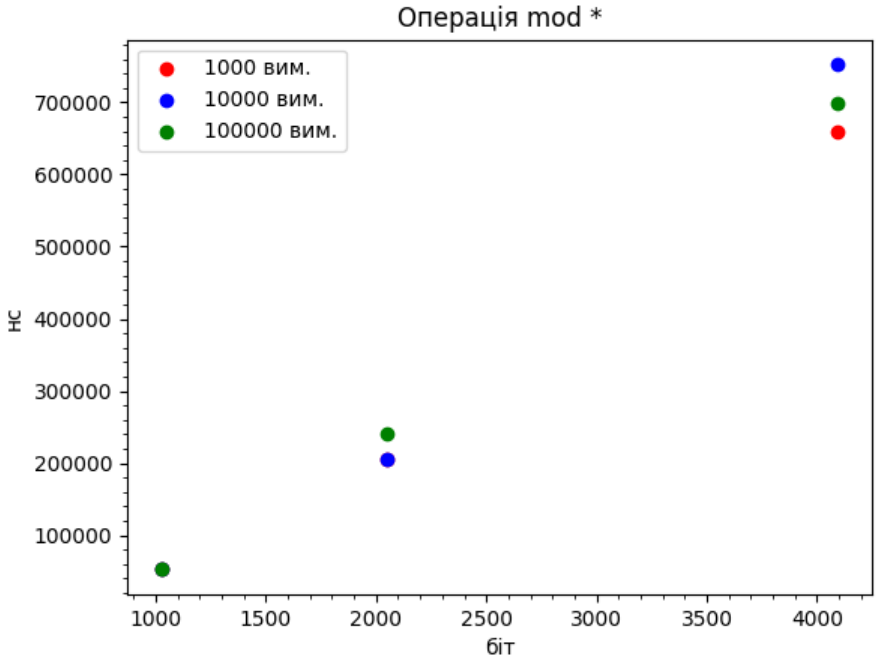
```
running 13 tests
test tests::power_mod_barret_test ... ok
test context::tests::mod_sub ... ok
test context::tests::mod_mul ... ok
test context::tests::mod_add ... ok
test tests::barret_reduction_test ... ok
test tests::equality_1 ... ok
test context::tests::mod_pow ... ok
test tests::equality_2 ... ok
test tests::lcm_test ... ok
test tests::gcd2_test ... ok
test tests::gcd1_test ... ok
test tests::equality_3_1 ... ok
test tests::equality_3_2 ... ok

test result: ok. 13 passed; 0 failed; 0 ignored; 0 measured; 0 filtered out; finished in 0.38s
```

Оцінка часу виконання операцій

Використовувалися випадкові значення модуля відповідної довжини.






Операція mod *
1000 вим.
10000 вим.
100000 вим.
700000
600000
500000
400000
300000
200000
100000
нс
1000
1500
2000
2500
3000
3500
4000
біт