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 .

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.

Б) Проконтролювати коректність реалізації алгоритмів; зокрема, для декількох Багаторозрядних a,b,c,n перевірити тотожності

В) Обчислити середній час виконання реалізованих арифметичних операцій. Підрахувати кількість тактів процесора (або інших одиниць виміру часу) на кожну операцію. Результати подати у вигляді таблиць або діаграм.

Хід роботи

Після до написання бібліотеки класу bignum, а саме функцій для роботи з модулярною арифметикою, створимо файл тестування що перевірить коректність нашої роботи. В ньому ми порівняємо значення обраховані за допомогою бібліотеки та без неї.

Демонстрація роботи:

```
gratigo@dedsec:~/Documents/term5/SROM/lab1/prikhodko_fb12_lab1/sources$ ipython3
^[[APython 3.10.12 (main, Jun 11 2023, 05:26:28) [GCC 11.4.0]
Type 'copyright', 'credits' or 'license' for more information
IPython 7.31.1 -- An enhanced Interactive Python. Type '?' for help.

In [1]: BITS = 2048

In [2]: from random import getrandbits

In [3]: A,B,C = getrandbits(BITS),getrandbits(BITS),getrandbits(BITS//2)

In [4]: from compmath.bn import *

In [5]: a,b = bn(A),bn(B)

In [6]: R = Ring(C)

In [7]: a = R(a)

In [8]: (a+b).base10()
Out[8]: 856998777877271952813457584044639173310586201525477715196689326362548667996820316065689792007897
422130799797128360136878137883286423238843190874303785754633370125713166001097554776928318709842299748307

In [9]: (a+b).base10() == (A+B)%C
Out[9]: True

In [10]: (a-b).base10() == (A-B)%C
Out[10]: True

In [11]: (a*b).base10() == (A*B)%C
Out[11]: True

In [12]: (a**b).base10() == pow(A,B,C)
Out[12]: True
```

Проведемо тести, запишемо час, і запустимо профайлер.

```
gratigo@dedsec:~/Documents/term5/SROM/lab1/prikhodko_fb12_lab1/sources$ ./tests.py
[*] Checking the correctness of the convertion...
A == Abn: True
A16== Abn16: True
A2 == Abn2: True
[!] Convertion to common bases seeems right
[*] Checking addition...
A + B == Abn + Bbn (mod C): True
[!] Addition seems right checking subtraction...
A - B == Abn - Bbn: True
[!] Subtraction seems right
[*] Checking multiplication...
A * B == Abn * Bbn: True
(Abn+Bbn)*Cbn == Abn*Cbn + Bbn*Cbn: True
[!] Multiplication seems right
[*] Checking power...
Abn**Bbn == A**B: True
gratigo@dedsec:~/Documents/term5/SROM/lab1/prikhodko_fb12_lab1/sources$
```

Додавання

```
       119 function calls in 0.001 seconds

 Ordered by: standard name

 ncalls  tottime  percall  cumtime  percall filename:lineno(function)
      1    0.000    0.000    0.001    0.001 <string>:1(<module>)
      1    0.000    0.000    0.000    0.000 __init__.py:384(__getattr__)
      1    0.000    0.000    0.000    0.000 __init__.py:391(__getitem__)
      2    0.001    0.000    0.001    0.000 bn.py:155(__mod__)
      2    0.000    0.000    0.000    0.000 bn.py:207(__le__)
      2    0.000    0.000    0.000    0.000 bn.py:225(__lt__)
      8    0.000    0.000    0.000    0.000 bn.py:229(__eq__)
      7    0.000    0.000    0.000    0.000 bn.py:33(__init__)
      2    0.000    0.000    0.001    0.000 bn.py:335(__init__)
      1    0.000    0.000    0.001    0.001 bn.py:339(__add__)
      1    0.000    0.000    0.000    0.000 bn.py:41(__add__)
      7    0.000    0.000    0.000    0.000 bnTypes.py:15(convert)
      2    0.000    0.000    0.000    0.000 bnTypes.py:3(getDigits)
      1    0.000    0.000    0.001    0.001 prof_tests.py:10(add)
      1    0.000    0.000    0.001    0.001 {built-in method builtins.exec}
     13    0.000    0.000    0.000    0.000 {built-in method builtins.isinstance}
     37    0.000    0.000    0.000    0.000 {built-in method builtins.len}
      3    0.000    0.000    0.000    0.000 {built-in method builtins.max}
      2    0.000    0.000    0.000    0.000 {built-in method builtins.min}
      1    0.000    0.000    0.000    0.000 {built-in method builtins.setattr}
      1    0.000    0.000    0.000    0.000 {method 'disable' of '_lsprof.Profiler' objects}
     22    0.000    0.000    0.000    0.000 {method 'pop' of 'list' objects}
      1    0.000    0.000    0.000    0.000 {method 'startswith' of 'str' objects}


       106 function calls in 0.001 seconds

 Ordered by: standard name
```

Віднімання:

```
       106 function calls in 0.001 seconds

 Ordered by: standard name

 ncalls  tottime  percall  cumtime  percall filename:lineno(function)
      1    0.000    0.000    0.001    0.001 <string>:1(<module>)
      2    0.001    0.000    0.001    0.000 bn.py:155(__mod__)
      2    0.000    0.000    0.000    0.000 bn.py:207(__le__)
      2    0.000    0.000    0.000    0.000 bn.py:225(__lt__)
      7    0.000    0.000    0.000    0.000 bn.py:229(__eq__)
      7    0.000    0.000    0.000    0.000 bn.py:33(__init__)
      2    0.000    0.000    0.001    0.000 bn.py:335(__init__)
      1    0.000    0.000    0.001    0.001 bn.py:346(__sub__)
      1    0.000    0.000    0.000    0.000 bn.py:41(__add__)
      2    0.000    0.000    0.000    0.000 bn.py:64(__sub__)
      1    0.000    0.000    0.000    0.000 bn.py:9(compare)
      7    0.000    0.000    0.000    0.000 bnTypes.py:15(convert)
      1    0.000    0.000    0.000    0.000 bnTypes.py:3(getDigits)
      1    0.000    0.000    0.001    0.001 prof_tests.py:12(sub)
      1    0.000    0.000    0.001    0.001 {built-in method builtins.exec}
     13    0.000    0.000    0.000    0.000 {built-in method builtins.isinstance}
     33    0.000    0.000    0.000    0.000 {built-in method builtins.len}
      3    0.000    0.000    0.000    0.000 {built-in method builtins.max}
      1    0.000    0.000    0.000    0.000 {built-in method builtins.min}
      1    0.000    0.000    0.000    0.000 {method 'disable' of '_lsprof.Profiler' objects}
     17    0.000    0.000    0.000    0.000 {method 'pop' of 'list' objects}
```

Множення

```
      139 function calls in 0.001 seconds

Ordered by: standard name

ncalls  tottime  percall  cumtime  percall filename:lineno(function)
     1    0.000    0.000    0.001    0.001 <string>:1(<module>)
     2    0.001    0.001    0.001    0.001 bn.py:155(__mod__)
     2    0.000    0.000    0.000    0.000 bn.py:207(__le__)
     2    0.000    0.000    0.000    0.000 bn.py:225(__lt__)
     8    0.000    0.000    0.000    0.000 bn.py:229(__eq__)
     7    0.000    0.000    0.000    0.000 bn.py:33(__init__)
     2    0.000    0.000    0.001    0.001 bn.py:335(__init__)
     1    0.000    0.000    0.001    0.001 bn.py:353(__mul__)
     1    0.000    0.000    0.000    0.000 bn.py:98(__mul__)
     7    0.000    0.000    0.000    0.000 bnTypes.py:15(convert)
     2    0.000    0.000    0.000    0.000 bnTypes.py:3(getDigits)
     1    0.000    0.000    0.001    0.001 prof_tests.py:14(mul)
     1    0.000    0.000    0.001    0.001 {built-in method builtins.exec}
    12    0.000    0.000    0.000    0.000 {built-in method builtins.isinstance}
    49    0.000    0.000    0.000    0.000 {built-in method builtins.len}
     4    0.000    0.000    0.000    0.000 {built-in method builtins.max}
     2    0.000    0.000    0.000    0.000 {built-in method builtins.min}
     1    0.000    0.000    0.000    0.000 {method 'disable' of '_lsprof.Profiler' objects}
    34    0.000    0.000    0.000    0.000 {method 'pop' of 'list' objects}
```

Степінь:

```
      548423 function calls in 0.605 seconds

Ordered by: standard name

ncalls  tottime  percall  cumtime  percall filename:lineno(function)
     1    0.000    0.000    0.605    0.605 <string>:1(<module>)
     2    0.000    0.000    0.000    0.000 __init__.py:384(__getattr__)
     2    0.000    0.000    0.000    0.000 __init__.py:391(__getitem__)
     1    0.000    0.000    0.000    0.000 bn.py:155(__mod__)
  3069    0.002    0.000    0.005    0.000 bn.py:197(__ge__)
     1    0.000    0.000    0.000    0.000 bn.py:207(__le__)
     1    0.000    0.000    0.000    0.000 bn.py:225(__lt__)
  3075    0.001    0.000    0.001    0.000 bn.py:229(__eq__)
     1    0.000    0.000    0.001    0.001 bn.py:25(conv)
 15351    0.014    0.000    0.050    0.000 bn.py:33(__init__)
     1    0.000    0.000    0.000    0.000 bn.py:335(__init__)
     1    0.003    0.003    0.605    0.605 bn.py:361(__pow__)
  3069    0.027    0.000    0.520    0.000 bn.py:392(barrettReduction)
  3069    0.081    0.000    0.103    0.000 bn.py:64(__sub__)
  3070    0.002    0.000    0.002    0.000 bn.py:9(compare)
  9207    0.411    0.000    0.449    0.000 bn.py:98(__mul__)
 15351    0.032    0.000    0.034    0.000 bnTypes.py:15(convert)
    36    0.000    0.000    0.001    0.000 bnTypes.py:3(getDigits)
     1    0.000    0.000    0.605    0.605 prof_tests.py:16(pow)
     1    0.000    0.000    0.605    0.605 {built-in method builtins.exec}
 33769    0.003    0.000    0.003    0.000 {built-in method builtins.isinstance}
190319    0.010    0.000    0.010    0.000 {built-in method builtins.len}
 21483    0.003    0.000    0.003    0.000 {built-in method builtins.max}
     2    0.000    0.000    0.000    0.000 {built-in method builtins.setattr}
  2016    0.000    0.000    0.000    0.000 {method 'append' of 'list' objects}
     1    0.000    0.000    0.000    0.000 {method 'disable' of '_lsprof.Profiler' objects}
245521    0.015    0.000    0.015    0.000 {method 'pop' of 'list' objects}
     2    0.000    0.000    0.000    0.000 {method 'startswith' of 'str' objects}
```