НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ім. Ігоря СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Комп'ютерний практикум №1 з курсу
Методи Реалізації Криптографічних Механізмів

Реалізація алгоритмів арифметики великих чисел (багатократної точності) над скінченими полями та групами

Виконав студент
групи ФІ-22мн
Кушнір О.С.

Перевірив:
асистент
Селюх П.В.

Київ — 2022

1 МЕТА КОМП'ЮТЕРНОГО ПРАКТИКУМУ

Дослідження алгоритмів реалізації арифметичних операцій над великими (багато розрядними) числами над скінченими полями та групами з точки зору їх ефективності за часом та пам'яттю для різних програмно-апаратних середовищ.

2 ПОСТАНОВКА ЗАДАЧІ

В даному комп'ютерному практикумі пропонуэться дослідити стандартну бібліотеку багатослівної арифметики Pari/GP, а саме функції багато розрядної арифметики обраної бібліотеки з описом алгоритму, вхідних та вихідних даних, кодів повернення. Контрольний приклад роботи з функціями.

3 ХІД РОБОТИ

Наведемо перелік методів бібліотеки, що стосуються арифметики великих чисел над скінченними полями.

randomprime(x)

Вхід:

x: t_INT | t_VEC - верхня межа інтервалу (тобто ми можемо передати 2^n) або ж вектор що складається з верхньої та нижньої межі (якщо не знайде простого може піти у нескінченний цикл).

Вертає:

p: t_INT - сильне псевдопросте число (це число яке проходить сильну версію тесту простоти), або ж просте число, якщо $x < 2^{64}$.

Приклад:

```
p = randomprime(2^100)
%1 = 792438309994299602682608069491
```

Mod(n, m)

Вхід:

n: t_INT | t POL - ціле число або поліном. m: t_INT - ціле число.

Вертає:

a: t_INTMOD | t_POLMOD - число або поліном n за модулем m.

Приклад:

```
a = Mod(2, 792438309994299602682608069491)
type(a)
%1 = "t_INTMOD"
a.mod
%2 = 792438309994299602682608069491
```

ffgen(n, x)

Вхід:

n: t_INT | t_VEC - ціле число, яке є степінем простого числа, або вектор [t,f], де t - просте число, f - степінь. x: t_POL - ціле число

Вертає:

g: t_FFELT - генератор елементів поля.

Приклад:

```
g = ffgen([2,4], 'x);
g.mod
%1 = x^4 + x^3 + x^2 + x + 1
g.f
%2 = 4
g.p
%3 = 2
type(g)
%4 = "t_FFELT"
```

random(g)

Вхід:

g: t_FFELT - генератор елементів поля

Вертає:

g: t_FFELT - випадковий елемент поля.

Приклад:

```
g = ffgen([2,4], 'x);
d = random(g)
%1 = x^3
type(d)
%2 = "t_FFELT"
```

issquare(g)

Вхід:

g: t_FFELT - елемент поля.

Вертає:

b: t_INT - приймає значення виключно 0 якщо g не має квадратичних лишків, або ж 1 якщо має, тобто з числа g можна взяти квадратний корінь за модулем.

Приклад:

```
g = ffgen([2,4], 'x);
d = random(g)
issquare(d)
```

```
%1 = 1
```

trace(d)

Вхід:

d: t_FFELT - елемент поля.

Вертає:

b: t_INT - слід елемента.

Приклад:

```
g = ffgen([2,4], 'x);
d = random(g)
trace(d)
%1 = Mod(1, 2)
```

norm(d)

Вхід:

d: t_FFELT - елемент поля.

Вертає:

b: t_INT - норма елемента.

Приклад:

```
g = ffgen([2,4], 'x);
d = random(g)
norm(d)
%1 = Mod(1, 2)
```

norm(d)

Вхід:

d: t_FFELT - елемент поля.

Вертає:

b: t_INT - норма елемента.

Приклад:

```
g = ffgen([2,4], 'x);
d = random(g)
norm(d)
```

```
%1 = Mod(1, 2)
```

minpoly(d)

Вхід:

d: t_FFELT - елемент поля.

Вертає:

b: t_INT - мінимальний поліном.

Приклад:

```
g = ffgen([2,4], 'x);
d = random(g)
minpoly(d)
%1 = Mod(1, 2)*x^4 + Mod(1, 2)*x^3 + Mod(1, 2)
```

factor(a)

Вхід:

a: t_INT | t POL - ціле число або поліном.

Вертає:

b: t_MAT - матриця з векторів, де кожен вектор вида [p, q] такий, що p - простий множник, а q - це його степінь.

Приклад:

```
g = ffgen([2,4], 'x);
d = random(g)
minpoly(d)
%1 = Mod(1, 2)*x^4 + Mod(1, 2)*x^3 + Mod(1, 2)
```

Опис:

Це функція факторизації для числа або ж полінома.

polrootsmod(p)

Вхід:

p: t POL - поліном.

Вертає:

r: t_COL - корені многочлену p над полем Галуа, у вигляді колоночного вектора.

Приклад:

```
c = ffgen(3^8,'c)
%1 = c
r = polrootsmod(x^7+x+c)
%1 = [c^7 + 2*c^6 + c^5 + c^3 + 2*c + 2, 2*c^7 + c^6 + c^2 + 1]~
```

fforder(c)

Вхід:

c: t_FFELT - елемент поля.

Вертає:

o: t_INT - порядок елементу.

Приклад:

```
c = ffgen(3^8,'c)
%1 = c
o = fforder(c)
%1 = 1640
```

ffprimroot(c)

Вхід:

c: t_FFELT - елемент поля.

Вертає:

o: t_INT | t_POL - примітивний корінь мультиплікативної групи поля.

Приклад:

```
c = ffgen(3^8,'c)
%1 = c
o = ffprimroot(c)
%1 = c^7 + 2*c^6 + c^3 + c^2 + c + 1
```

fflog(c,o)

Вхід:

c: t_FFELT - елемент поля. o: t_INT | t_POL - примітивний корінь мультиплікативної групи поля.

Вертає:

l: t_INT - дискретный логарифм элементу поля Галуа, $c = o^n$.

Приклад:

```
c = ffgen(3^8,'c)
%1 = c
o = ffprimroot(c)
%2 = c^7 + 2*c^6 + c^5 + 2*c^3 + c^2
n = fflog(c,o)
%3 = 5636
o^n
%4 = c
```

ВИСНОВКИ

Під час виконання практикуму було виконане ознайомлення з методами бібліотеки Pari/GP, виконано опис методів бібліотеки що стосуються скінченних полей. Як видно з опису бібліотека Pari/GP має всі необхідні методи для виконання операцій над скінченними полями та групами і може ефективно працювати незалежно від програмно-апаратного середовища, але має обмеження в архітектурах Windows та на малих апаратних потужностях.