Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Звіт
до ЛАБОРАТОРНОЇ РОБОТА №2
з дисципліни: “Спеціальні розділи обчислювальної математики”

Виконала студентка:
групи ФІ-03
Швець Катерина

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

Реалізувати редукцію Барретта використовуючи клас BigInteger з лабораторної роботи 1

Псевдокод:

q := right_shift(x, k-1);
q := q * ;
q := right_shift(q, k+1);
r := x – q * n;
while (r >= n) do:
r := r – n;
return r;

Вхідні дані: 285276 mod 543
Результат: 201
In hex вхідні дані: 45a5c mod 21f
Результат 9c

Код програми:

```
def BarrettReduction(self, n):
    c=BigInteg("1")
    k= n.elder_bit()+1
        #m=c.left_shift(2*k).LongDivMod(n)
    m=BigInteg("733")
    q= self.right_shift(k-1)
    q=BigInteg(q)
    q = q*m
    q=BigInteg(q)
    q= q.right_shift(k+1)
    q=BigInteg(q)
    a=q*n
    a=BigInteg(a)
    r=self-a
    r=BigInteg(r)
    while(r.LongCmp(n)!=-1):
        r-=n
        r=BigInteg(r)
    return r.n
```

```
a=BigInteg("45a5c")
b=BigInteg("21f")
print(a.BarrettReduction(b))
```

Результат: