

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №8

Тема: Целочисленная арифметика многократной точности

дисциплина: Математические основы защиты информации и информационной безопасности

Студент: Койфман Кирилл Дмитриевич

Группа: НФИмд-01-25

Введение

Цель работы

Получение практических навыков реализации алгоритмов, выполняющих арифметические операции с большими целыми числами.

Задачи

1. Реализовать алгоритмы, выполняющие арифметические операции с большими целыми числами.
2. Протестировать работу реализованных алгоритмов.

Ход работы

1 задание

Для решения поставленной задачи реализуем описанные в тексте лабораторной работы алгоритмы, выполняющих арифметические операции с большими целыми числами, на языке программирования C++ (Листинг-1):

```
//algorithm 1: addition of non-negative integers
Value algorithm_1(const Value& u, const Value& v, int b)
{
    //define max number of digits
    int n = std::max(u.size(), v.size());

    //define the result value
    Value w(n + 1, 0);
    int k = 0;

    //main cycle
    for (int i = 0; i < n; ++i)
    {
        int sum = k;

        if (i < u.size())
            sum += u[i];

        if (i < v.size())
            sum += v[i];

        w[i] = sum % b;
        k = sum / b;
    }
    w[n] = k;
    normalize(w);

    return w;
}

//algorithm 2: subtraction of non-negative integers
Value algorithm_2(const Value& u, const Value& v, int b)
{
    //define the result value and init borrow value
    Value w = u;
    int k = 0;

    //main cycle
    for (size_t i = 0; i < w.size(); ++i)
    {
        w[i] -= k;

        if (i < v.size())
            w[i] -= v[i];

        if (w[i] < 0)
```

```
        {
            k = 1;
            w[i] += b;
        }
        else
            k = 0;
    }
    normalize(w);

    return w;
}

//algorithm 3: column multiplication of non-negative integers
Value algorithm_3(const Value& u, const Value& v, int b)
{
    //define sizes number of digits for each of two values
    int n = u.size();
    int m = v.size();
    //define result value
    Value w(n + m, 0);

    //main cycle
    for (int j = 0; j < m; ++j)
    {
        if (v[j] == 0)
        {
            w[j] = 0;
            continue;
        }

        int k = 0;

        for (int i = 0; i < n; ++i)
        {
            int t = u[i] * v[j] + w[i + j] + k;
            w[i + j] = t % b;
            k = t / b;
        }

        w[n + j] = k;
    }
    normalize(w);

    return w;
}

//algorithm 4: fast column multiplication of non-negative integers
Value algorithm_4(const Value& u, const Value& v, int b)
{
    //define sizes number of digits for each of two values
    int n = u.size();
    int m = v.size();
    //define result value
    Value w(n + m, 0);
```

```

    long long t = 0;

    //main cycle
    for (int s = 0; s < m + n; ++s)
    {
        for (int i = std::max(0, s - m + 1); i <= std::min(s, n - 1); ++i)
        {
            int j = s - i;

            if (j >= 0 && j < m)
                t += (long long)u[i] * v[j];
        }
        w[s] = t % b;
        t /= b;
    }
    normalize(w);

    return w;
}

```

Листинг-1(реализация алгоритмов, выполняющих арифметические операции с большими целыми числами)

2 задание

Далее протестируем работу данных алгоритмов (Листинг-2, Листинг-3):

```

int main()
{
    std::cout << "\n-----Testing basic arithmetic
operations algorithms for big non-negative integers-----
----\n";

    //define system base number
    int b = g_b;

    //define init pair of big values with system base 'b'
    // 253
    Value u = { 3, 5, 2 };
    // 941
    Value v = { 1, 4, 9 };

    std::cout << "System base number b = " << b << "\nValue u = " << u <<
    ", value v = " << v << '\n';

    //conduct algorithms tests
    Value result_1 = algorithm_1(u, v, b);
    std::cout << "u + v = " << result_1 << '\n';

    Value result_2 = algorithm_2(v, u, b); // 456 - 123
}

```

```
std::cout << "v - u = " << result_2 << '\n';

Value result_3 = algorithm_3(u, v, b);
std::cout << "u * v (slow) = " << result_3 << '\n';

Value result_4 = algorithm_3(u, v, b);
std::cout << "u * v (fast) = " << result_4 << '\n';

std::cout << std::endl;

return 0;
}
```

Листинг-2(функция для проведения тестов алгоритмов)

```
-----Testing basic arithmetic operations algorithms
for big non-negative integers-----
System base number b = 10
Value u = 253, value v = 941
u + v = 1194
v - u = 688
u * v (slow) = 238073
u * v (fast) = 238073
```

Листинг-3(результаты проведенных тестов алгоритмов)

Заключение

В ходе проделанной лабораторной работы мной были получены навыки по реализации алгоритмов, выполняющих арифметические операции с большими целыми числами.