Лабораторная работа №8

Целочисленная арифметика произвольной точности

Студент: Хамза Хуссен

Цель: Изучение и программная реализация алгоритмов для выполнения арифметических операций над целыми числами, разрядность которых превышает возможности стандартных типов данных.

Введение в длинную арифметику

•**Что это?** Методы работы с числами, не помещающимися в стандартные типы данных (>128 бит).

•**Применение:** Криптография, компьютерная алгебра, точные научные расчёты.

•**Представление числа:**

- Основание системы счисления **b** (часто $b = 2^{32}, 2^{64}$).
- Число $X = (x_{n-1} \dots x_1 x_0)_b$, где $0 \le x_i < b$.
- Знак хранится отдельно.

Алгоритм сложения

Вход: Два n-разрядных числа u, v; основание b.

Выход: Сумма w = w_0 w_1 ... w_n (w_0 — перенос).

Шаги:

j = n, k = 0 (перенос).

w_j = (u_j + v_j + k) mod b; k = ⌊(u_j + v_j + k) / b⌋.

j--. Если j > 0 → шаг 2.

w_0 = k.

Алгоритм вычитания

- **Вход: u ≥ v; n-разрядные; основание b.**
- **Выход: Разность w = w_1 ... w_n.**
- **Шаги:**
- **j = n, k = 0 («заём»).**
- **w_j = (u_j - v_j + k) mod b; k = ⌊(u_j - v_j + k) / b⌋.**
- **j--. Если j > 0 → шаг 2.**

Алгоритм умножения «столбиком»

Вход: u (n разр.), v (m разр.); b.

Выход: w = u * v (m+n разр.).

Основные шаги:

Инициализация w нулями.

Внешний цикл по j (разряды v).

Внутренний цикл по i (разряды u) с накоплением переноса k.

Запись результата в w.

Алгоритм «быстрого столбика» (оптимизированное умножение)

1.Идея: Упрощение классического алгоритма за счёт группировки вычислений.

2.Шаги:

3.t = 0.

4.Для каждого s от 0 до m+n-1:

5.Суммирование произведений разрядов u и v, дающих текущий разряд результата.

6.w_{m+n-1-s} = t mod b; t = ⌊t / b⌋.

Алгоритм деления

Вход: Делимое u (n+1 разр.), делитель v (t+1 разр.), $n \geq t$, $v_t \neq 0$.

Выход: Частное q, остаток r.

Основные шаги:

Нормализация и подбор цифр частного.

Итеративное вычитание кратных делителя.

Коррекция цифры частного и остатка при необходимости.

Практическая реализация

Основание b: 10 (в учебных целях).

Что реализовано:

Сложение (Алгоритм 1).

Вычитание (Алгоритм 2).

Умножение «столбиком» (Алгоритм 3).

«Быстрый столбик» (Алгоритм 4).

Деление (Алгоритм 5).

Контрольный пример и тестирование

Пример: Операции с числами 12345 и 56789.

Цель тестов:

Проверка корректности результатов.

Сравнение работы разных алгоритмов (напр., стандартное и быстрое умножение).

Результат: Алгоритмы работают корректно, что подтверждается ручными расчётами.

Выводы

Итоги:

Освоены принципы хранения и обработки чисел произвольной точности.

Реализованы ключевые арифметические алгоритмы.

Получен опыт практического программирования длинной арифметики.

Значимость: Эти алгоритмы являются фундаментом для криптографии, защиты данных и других областей, требующих работы с очень большими целыми числами.