Отчёта по лабораторной работе №9

Отладчик GDB

Гомес Лопес Теофания

Содержание

# 1 Цель работы

Познакомиться с методами отладки при помощи GDB, его возможностями.

# 2 Выполнение лабораторной работы

## 2.1 Реализация подпрограмм в NASM

Создала каталог для программ ЛБ9, и в нем создала файл (рис. 1).

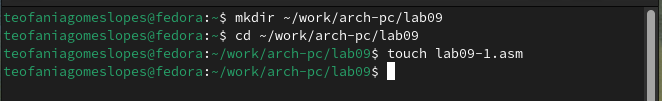


Рис. 1: Создала каталог с помощью команды mkdir и файл с помощью команды touch

Открывала файл в Midnight Commander и заполняла его в соответствии с листингом 9.1 (рис. 2).

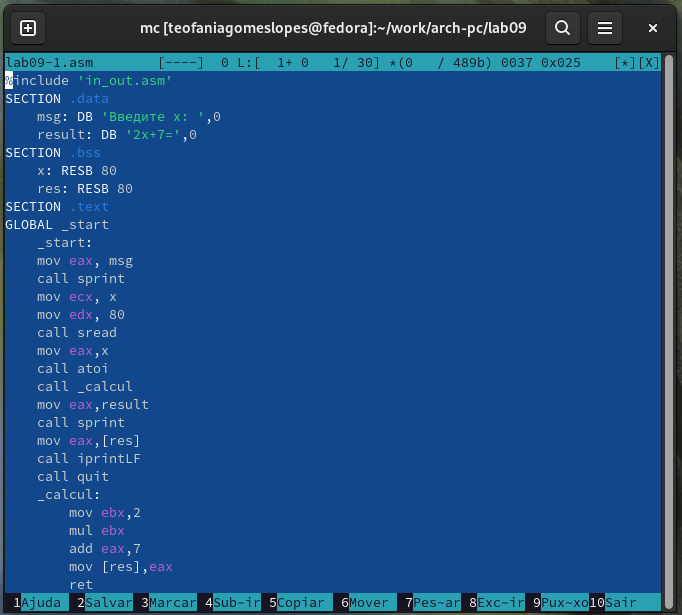


Рис. 2: Заполняла файл

Создала исполняемый файл и запускала его (рис. 3).

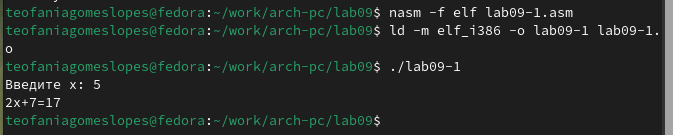


Рис. 3: Запускала файл и проверяла его работу

Снова открывала файл для редактирования и изменяла его, добавив подпрограмму в подпрограмму(по условию) (рис. 4).

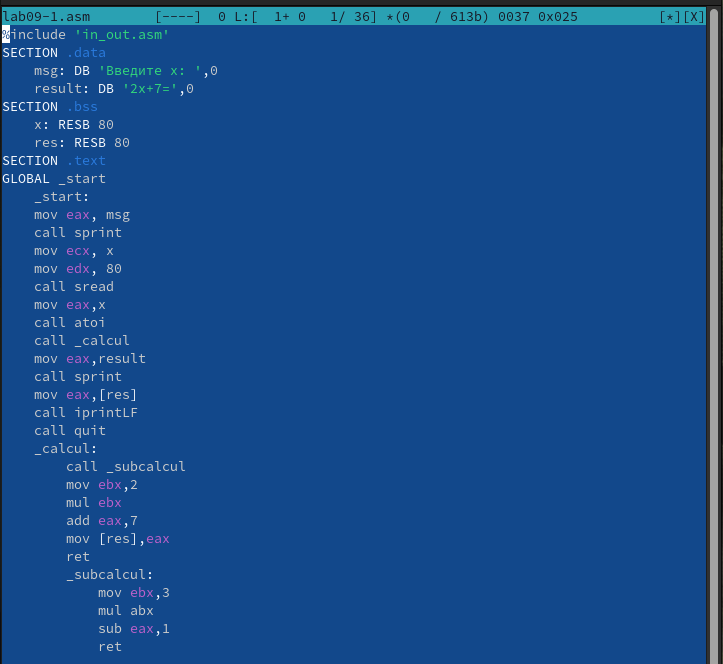


Рис. 4: Изменяла файл, добавляя еще одну подпрограмму

Создала исполняемый файл и запускала его (рис. 5).

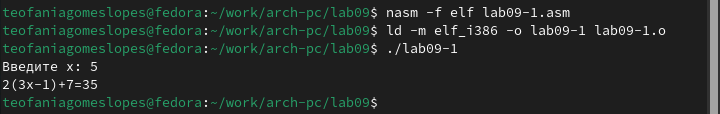


Рис. 5: Запускала файл и смотрела на его работу

## 2.2 Отладка программам с помощью GDB

Создала новый файл в каталоге (рис. 6).

Создала файл

Рис. 6: Создала файл

Открывала файл в Midnight Commander и заполняла его в соответствии с листингом 9.2 (рис. 7).

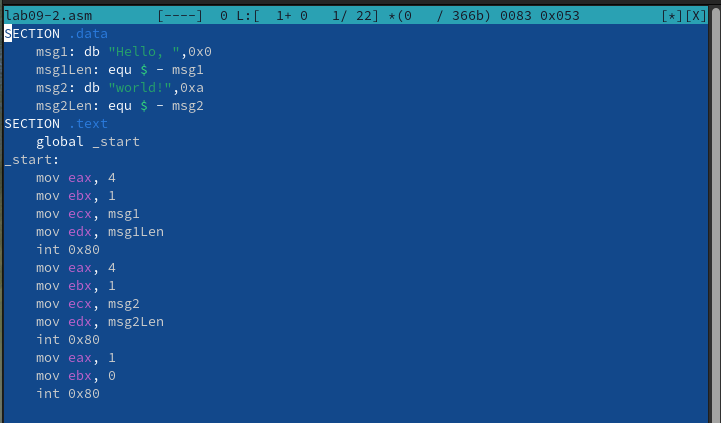


Рис. 7: Заполняла файл

Получала исходный файл с использованием отладчика gdb (рис. 8).

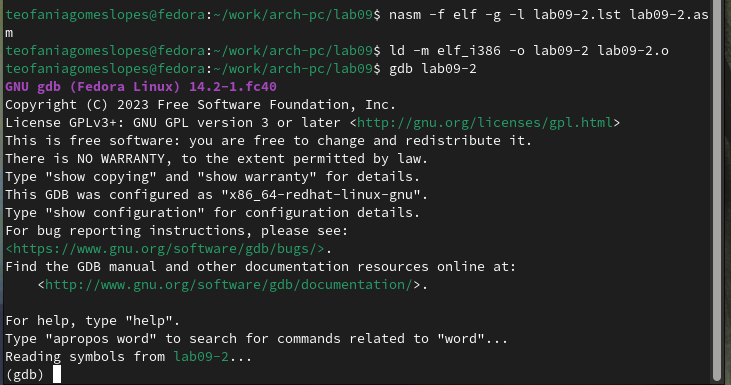


Рис. 8: Загружала исходный файл в отладчик

Запускала команду в отладчике (рис. 9).

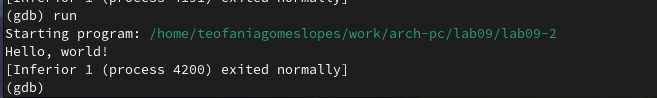


Рис. 9: Запускала программу командой run

Устанавливала брейкпоинт на метку \_start и запускала программу (рис. 10).



Рис. 10: Запускала программу с брейкпоином

Смотрела дисассимилированный код программы с помощью команды disassemble, начиная с метки \_start (рис. 11).



Рис. 11: Смотрела дисассимилированный код программы

Переключаемся на отображение команд с Intel’овским синтаксисом (рис. 12).



Рис. 12: Переключалась на синтаксис Intel

Различия отображения синтаксиса машинных команд в режимах ATT и Intel:

1.Порядок операндов: В ATT синтаксисе порядок операндов обратный, сначала указывается исходный операнд, а затем - результирующий операнд. В Intel синтаксисе порядок обычно прямой, результирующий операнд указывается первым, а исходный - вторым.

2.Разделители: В ATT синтаксисе разделители операндов - запятые. В Intel синтаксисе разделители могут быть запятые или косые черты (/).

3.Префиксы размера операндов: В ATT синтаксисе размер операнда указывается перед операндом с использованием префиксов, таких как “b” (byte), “w” (word), “l” (long) и “q” (quadword). В Intel синтаксисе размер операнда указывается после операнда с использованием суффиксов, таких как “b”, “w”, “d” и “q”.

4.Знак операндов: В ATT синтаксисе операнды с позитивными значениями предваряются символом “$". В Intel синтаксисе операнды с позитивными значениями могут быть указаны без символа "$”.

5.Обозначение адресов: В ATT синтаксисе адреса указываются в круглых скобках. В Intel синтаксисе адреса указываются без скобок.

Включала режим псевдографики (рис. 13).

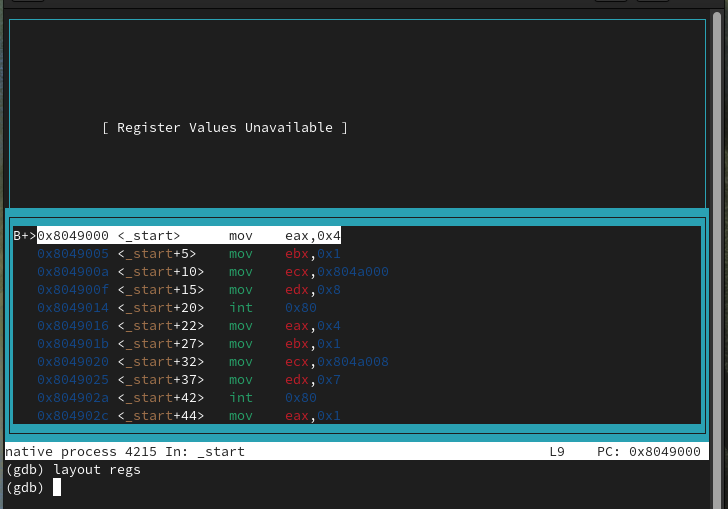


Рис. 13: Включала отображение регистров, их значений и результат дисассимилирования программы

Проверяла была ли установлена точка останова и устанавливала точку останова предпоследней инструкции (рис. 14).

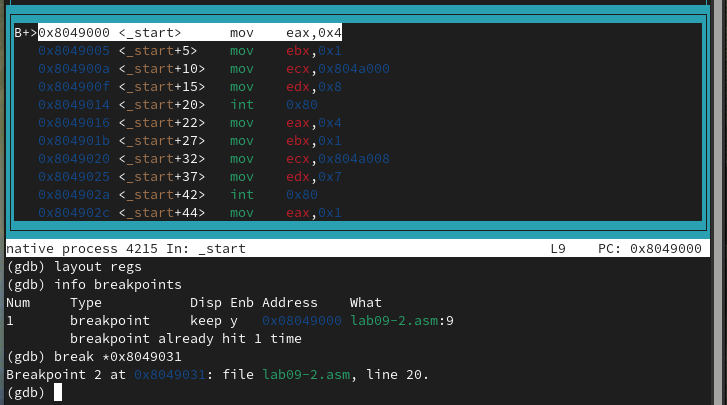


Рис. 14: Использовала команду info breakpoints и создала новую точку останова

Посмотрела информацию о всех установленных точках останова (рис. 15).

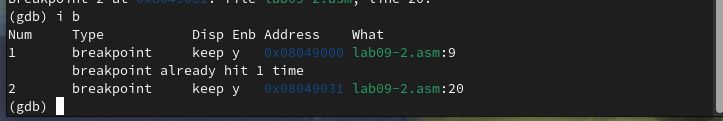


Рис. 15: Смотрела информацию

Выполняла 5 инструкций командой si (рис. 16).

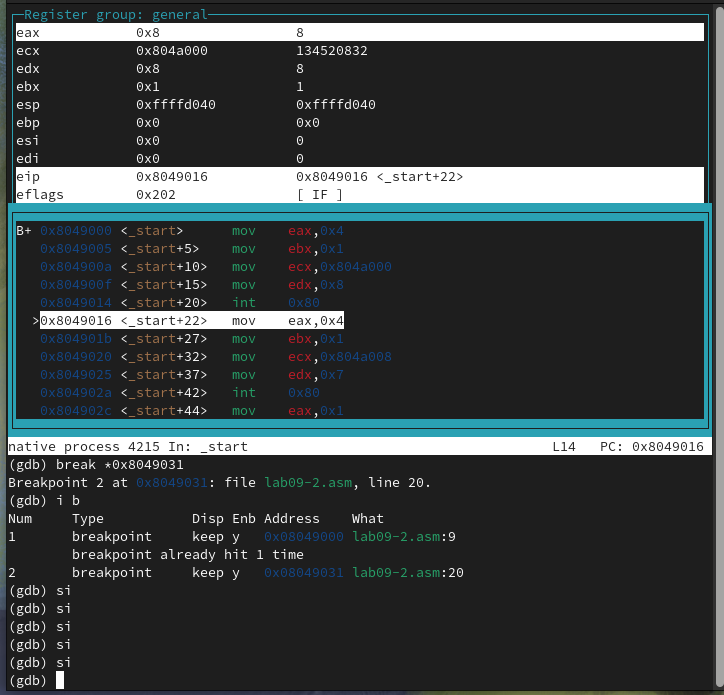


Рис. 16: Отслеживала регистры

Смотрела значение переменной msg1 по имени (рис. 17).

Смотрела значение переменной

Рис. 17: Смотрела значение переменной

Смотрела значение переменной msg2 по адресу (рис. 18).

Смотрела значение переменной

Рис. 18: Смотрела значение переменной

Изменила первый символ переменной msg1 (рис. 19).

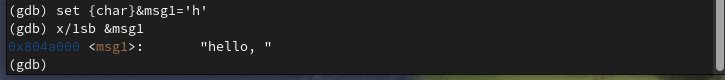


Рис. 19: Меняла символ

Изменила первый символ переменной msg2 (рис. 20).

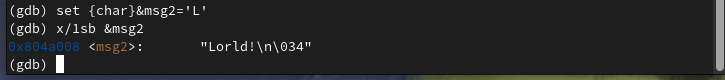


Рис. 20: Меняла символ

Смотрела значение регистра edx в разных форматах (рис. 21).

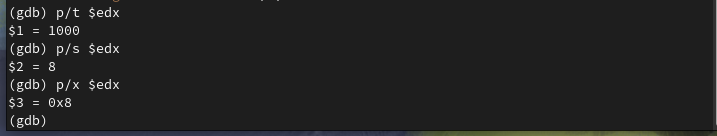


Рис. 21: Смотрела значение регистра

Изменяла регистор ebx (рис. 22).

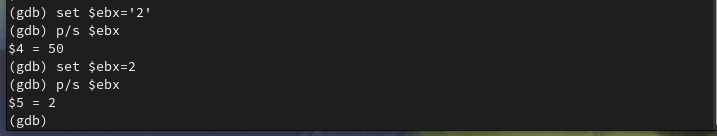


Рис. 22: Изменяла регистор командой set

Прописывала команды для завершения программы и выхода из GDB (рис. 23).

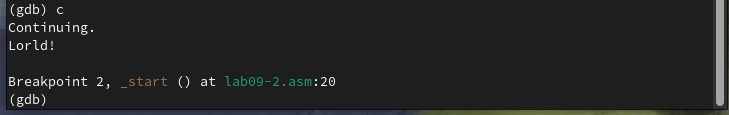


Рис. 23: Прописывала команды c и quit

Копировала файл lab8-2.asm в файл с именем lab09-3.asm (рис. 24).

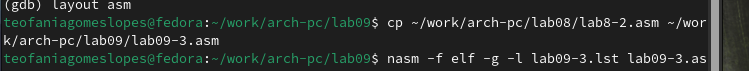


Рис. 24: Копировала файл

Создала исполняемый файл и запускала его в отладчике GDB (рис. 25).

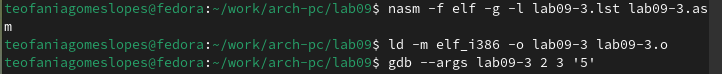


Рис. 25: Создала и запускала в отладчике файл

Установила точку останова перед первой инструкцией в программе и запустим ее (рис. 26).

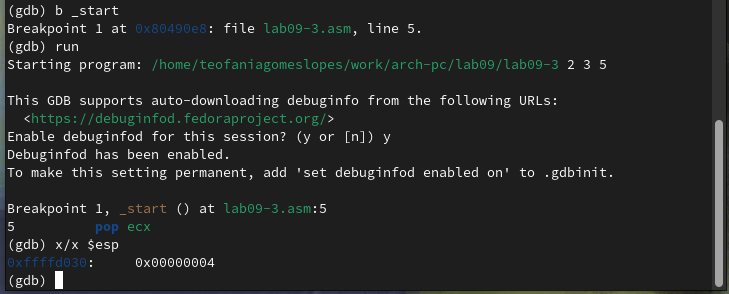


Рис. 26: Устанавливала точку останова

Смотрела позиции стека по разным адресам (рис. 27).

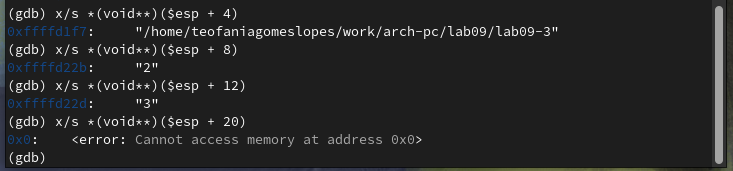


Рис. 27: Изучала полученные данные

Шаг изменения адреса равен 4 потому что адресные регистры имеют размерность 32 бита(4 байта).

##Задание для самостоятельной работы

###Задание 1

Копировала файл lab8-4.asm(ср №1 в ЛБ8) в файл с именем lab09-3.asm (рис. 28).

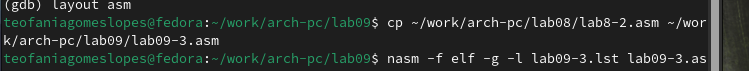


Рис. 28: Копировала файл

Открывала файл в Midnight Commander и меняла его, создавая подпрограмму (рис. 29).

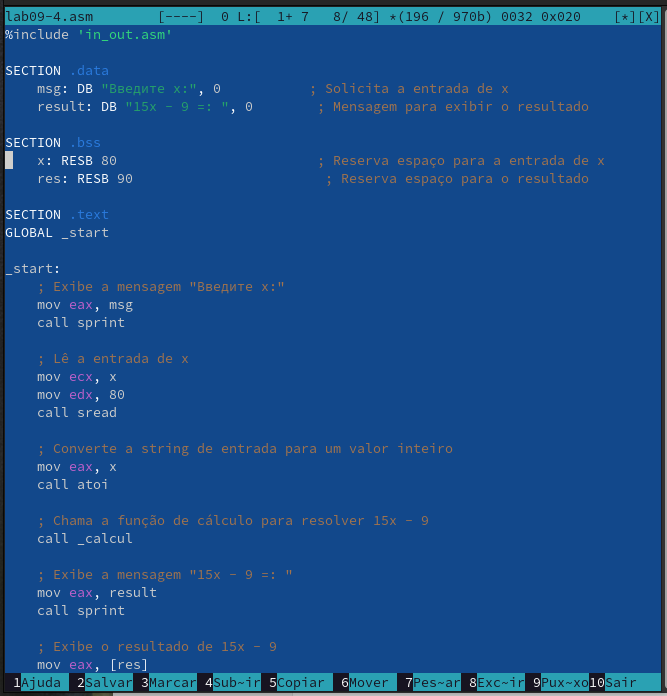


Рис. 29: Изменяла файл

Создала исполняемый файл и запускаем его (рис. 30).

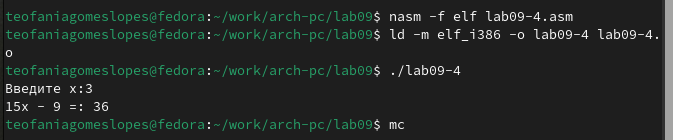


Рис. 30: Проверяем работу программы

###Задание 2

Создала новый файл в дирректории (рис. 31).

Создала файл

Рис. 31: Создала файл

Открывала файл в Midnight Commander и заполняем его в соответствии с листингом 9.3 (рис. 32).

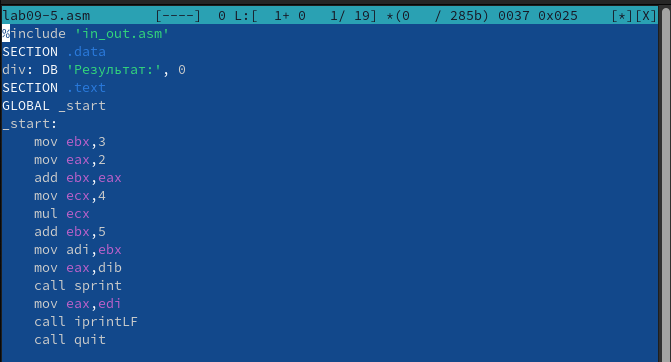


Рис. 32: Изменяла файл

Создала исполняемый файл и запускала его (рис. 33).

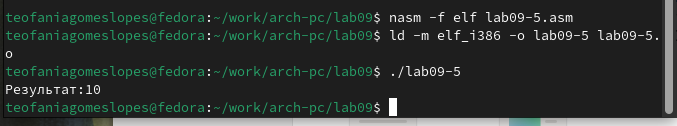


Рис. 33: Создала и смотрим на работу программы

Создала исполняемый файл и запускала его в отладчике GDB и смотрела на изменение решистров командой si (рис. 34).

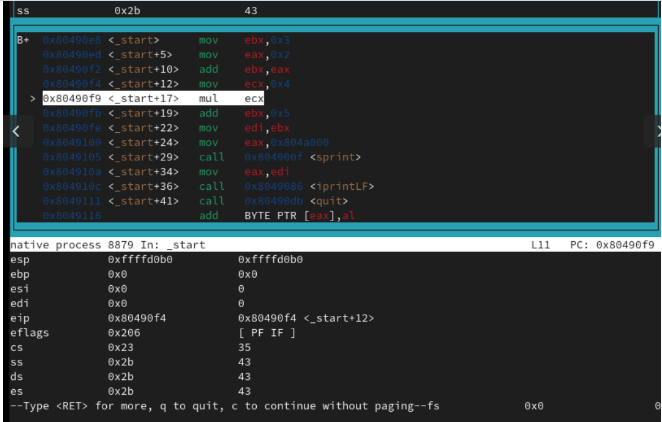


Рис. 34: Ищем ошибку регистров в отладчике

Изменяла программу для корректной работы (рис. 35)

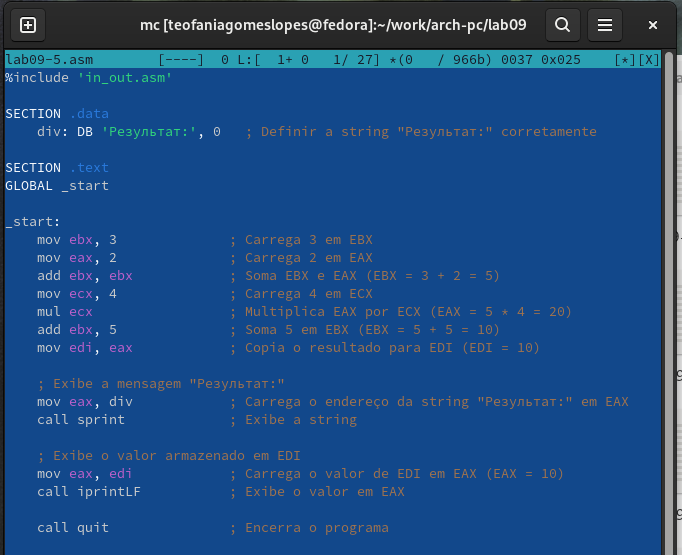


Рис. 35: Меняла файл

Создала исполняемый файл и запускала его (рис. 36)

|  |
| --- |
| Создала и запускала файл |

Рис. 36: Создала и запускала файл

# 3 Выводы

Мы познакомились с методами отладки при помощи GDB и его возможностями.

# Список литературы