Лабораторная работа №9

Понятие подпрограммы.Отладчик GDB.

Казначеев Сергей Ильич

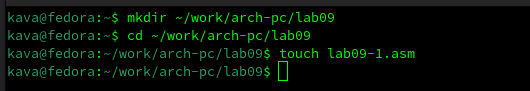
Содержание

# 1 Цель работы

Приобретение навыков написания программ с использованием подпрограмм. Знакомство с методами отладки при помощи GDB и его основными возможностями.

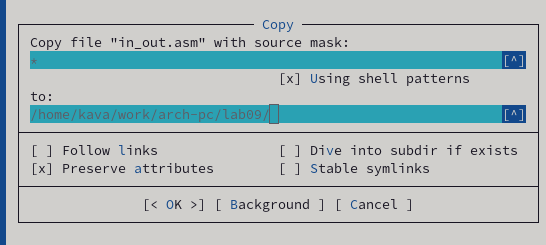
# 2 Выполнение лабораторной работы

Для начала создадим папку и файл lab9-1.asm



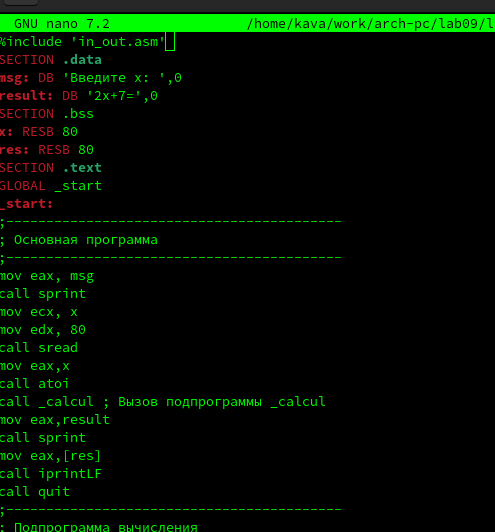
01

Далее, запустим Midnight commander и копируем файл in\_out.asm.



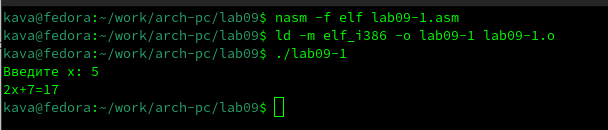
02

Вставляем в файл lab9-1.asm код из листинга 9.1



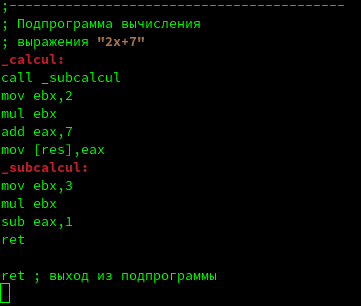
03

Собираем программу и проверяем её на корректность работы



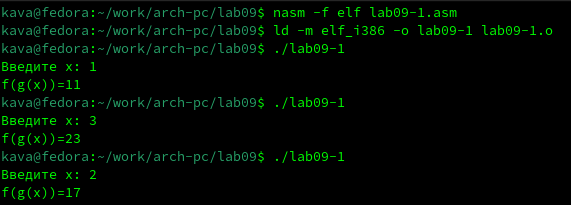
04

Теперь изменим файл так, чтобы внутри подпрограммы была ещё одна подпрограмма, вычисляющая значение g(x) и чтобы она передавала значение в первую подпрограмму, которая бы уже вычислила значение f(g(x))



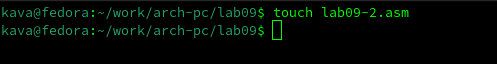
05

Собираем и проверяем



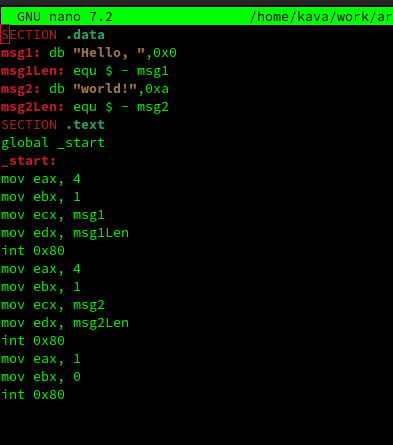
06

Создаем второй файл



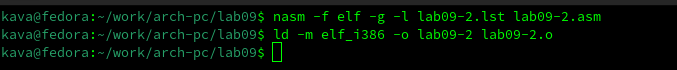
07

И вставляем код из листинга 9.2



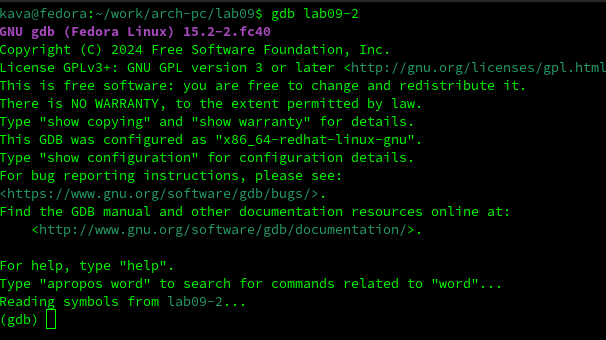
08

Соберем программу следующим образом



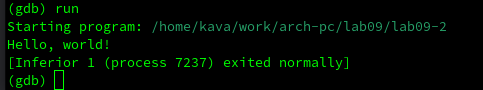
09

Теперь загружаем ее в gdb



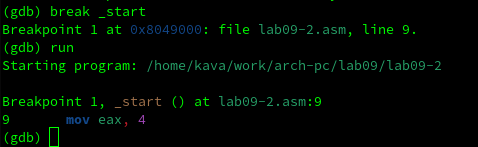
10

Запускаем ее с помощью команды run



11

Создадим брейкпоинт на метке \_start с помощью команды break



12

С помощью команды disassemble дизассемблируем её



13

Переключаем вывода синтекса на intel

14

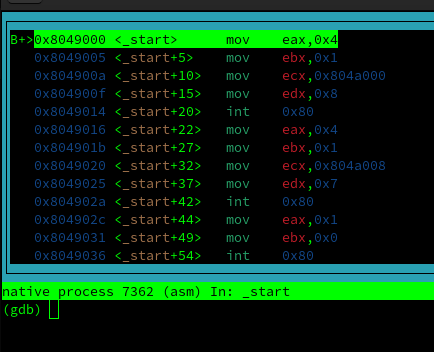
14

Повторяем команду disassemble



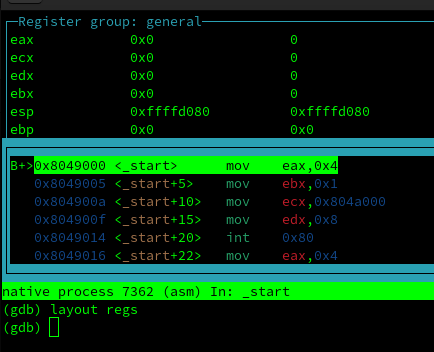
15

Включаем графическое отображение кода



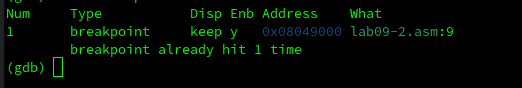
16

Теперь включаем графическое отображение значений регистров



17

Выводим всю информацию о всех брейкпоинтах



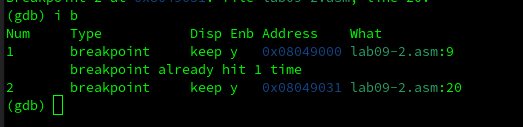
18

Создаем брейкпоинт по адресу

19

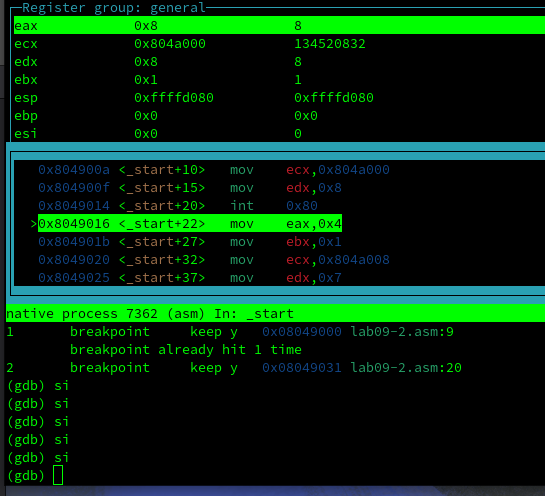
19

Выводим информацию



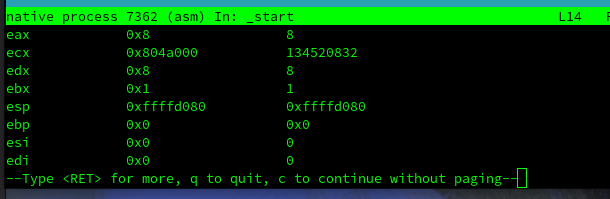
20

Теперь 5 раз выполняем команду si для построчного выполнения кода



21

Как видим, поменялись значения регистров eax, ecx, edx и ebx. Теперь выведем информацию о значениях регистров



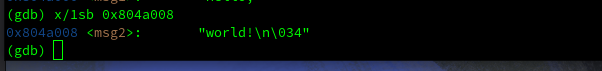
22

Выводим значения переменной по имени.



23

Теперь по адресу



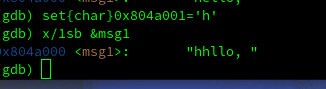
24

Теперь меняем первый символ



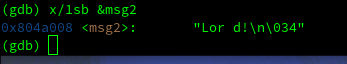
25

Меняем второй символ



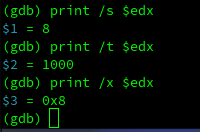
26

Меняем несколько символов второй переменной



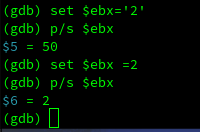
27

Выводим значения регистра в строковом,двоичном и шестнадцатиричном виде



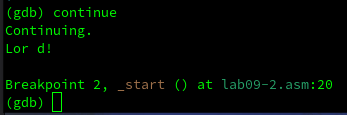
28

Пробуем изменить значения регистра



29

Мы увидим что в регистр записались разные значения, это связано с тем, что в одном случае мы записываем в него число, а в другом случае строчку. Завершаем программу с помощью команды continue и выйдем.



30

31

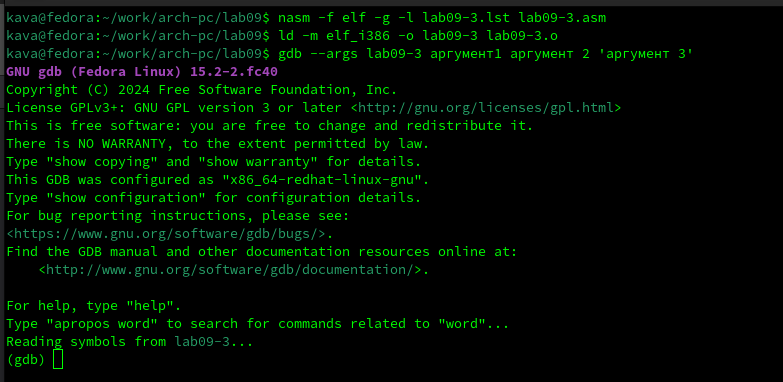
31

Копируем файл

32

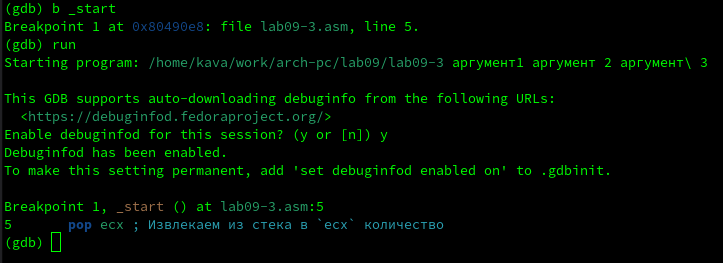
32

Соберём его и вгрузим в gdb



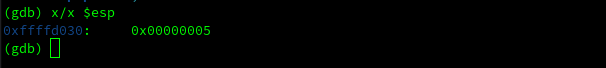
33

Создадим брейкпоинт и запустим программу



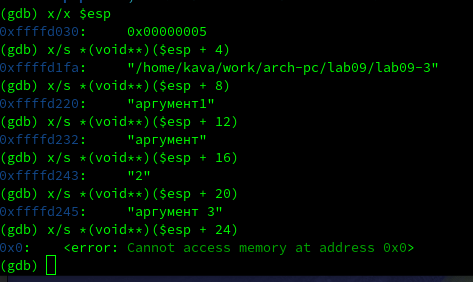
34

Выведем значение регистра esp, где хранятся данные о стеке



35

ВЫведем значения всех элементов стека

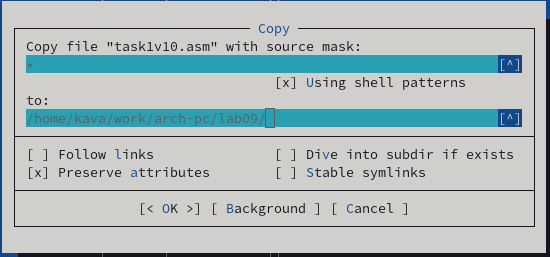


36

Как видим, для вывода каждого элемента стека нам нужно менять значение адреса с шагом 4. Это связано с тем, что именно с шагом 4 располагаются данные в стеке.

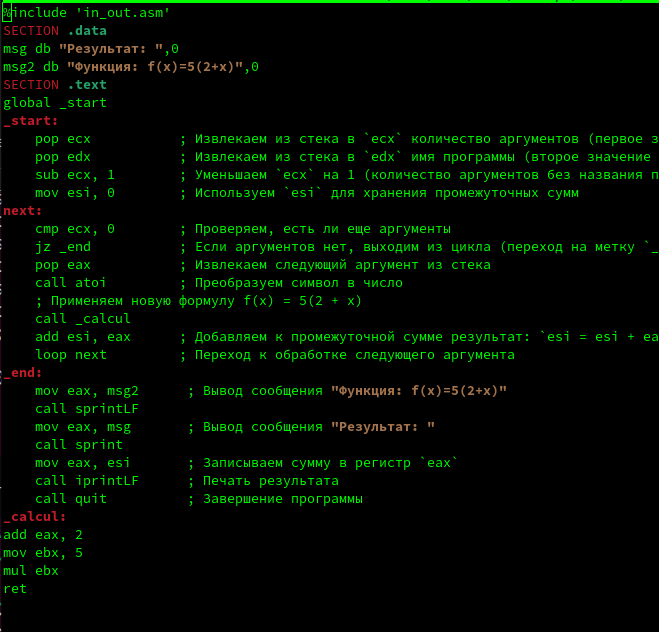
# 3 Выполнение заданий для самостоятельной работы

Копируем файл первого задания прошлой самостоятельной работы



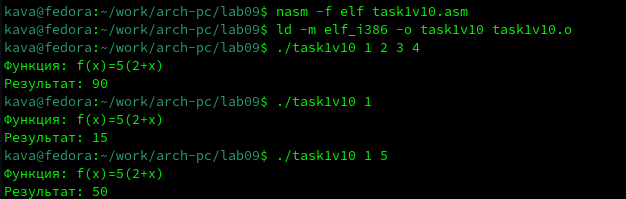
37

Переписываем так, чтобы он использовался для авчисления выражения подпрограммы



38

Собираем и проверяем на корректность выполнения.



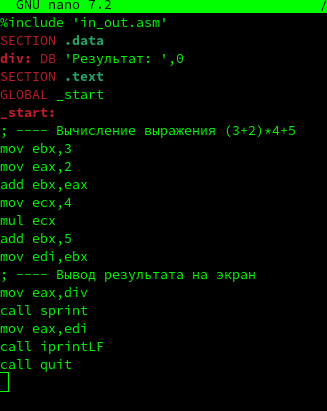
39

Создадим файл второго задания самостоятельной работы

40

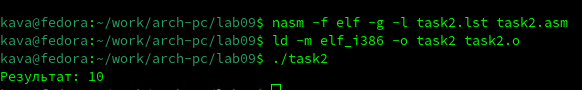
40

Далее вставляем код из листинга 9.3



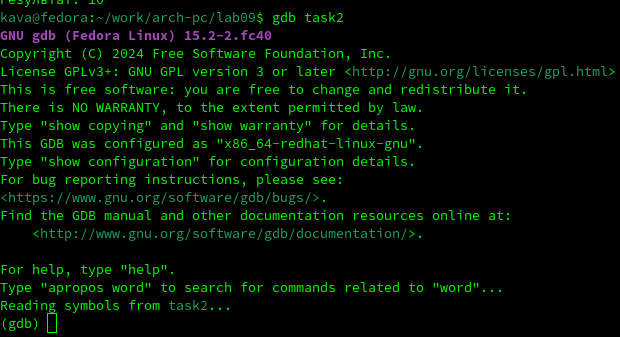
41

Собираем и запускуаем



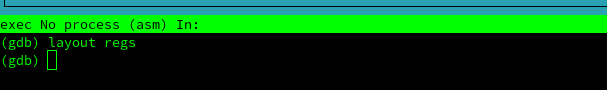
42

Как видим, код считает значение выражения неправильно. Загрузим его в gdb.



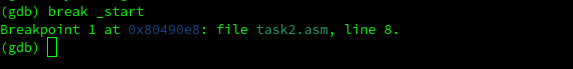
43

Включеним графическое отображение значений регистров и отображение графического отображения кода.



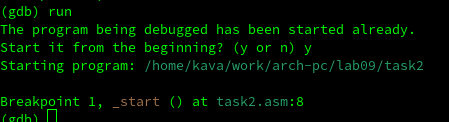
44

Устанавливаем брейкпоинт на \_start

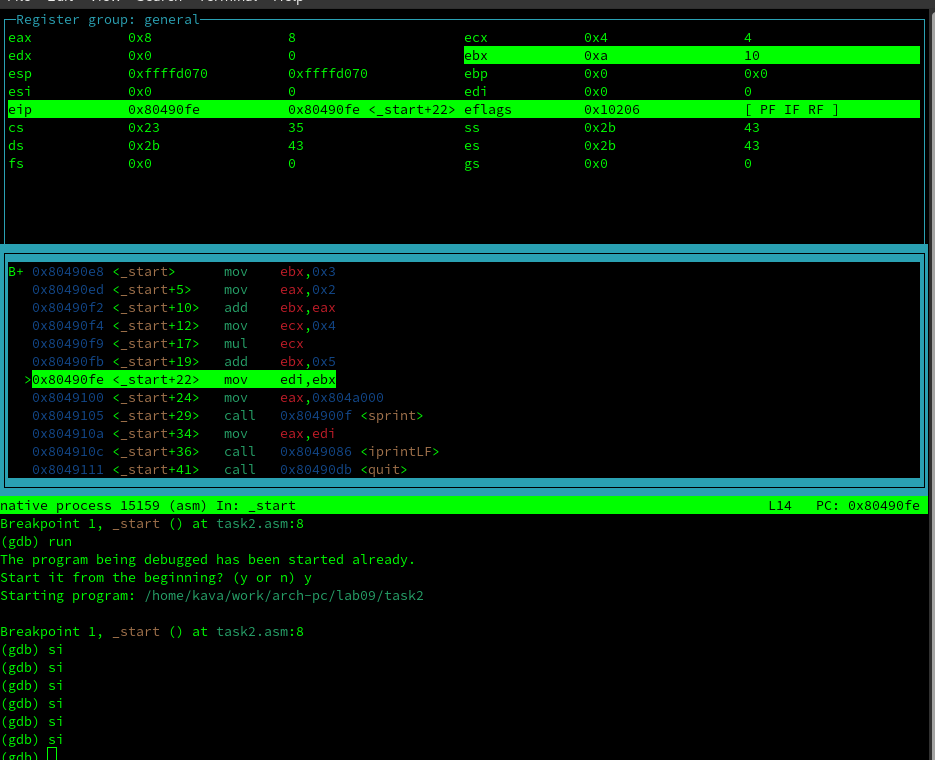


45

Запускаем и начинаем построчно выполнять код

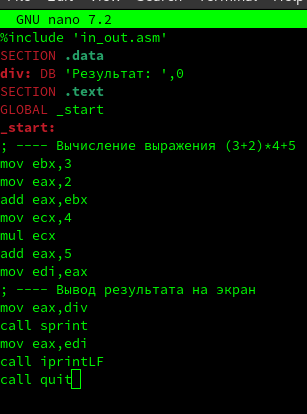


46



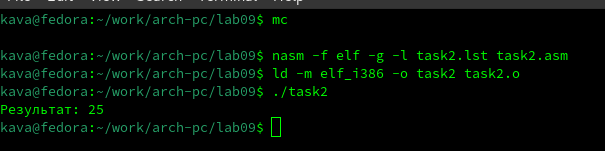
47

Как видим, мы должны были умножить значение регистра ebx, но умножили регистр eax. Нам необходимо все результаты хранить в регистре eax. Изменим код



48

И проверяем на корректность выполнения.



49

Как видим, теперь код работает корректно

# 4 Выводы

После выполнения лабораторной работы. Я приобрел навыки программ с использованием подпрограмм и познакомился с методами отладки при помощи GDB и его основными возможностями