Отчёт по лабораторной работе 9

Понятие подпрограммы. Отладчик GDB.

Скобеева Алиса Алексеевна

Содержание

# 1 Цель работы

Целью работы является приобретение навыков написания программ с использованием подпрограмм. Знакомство с методами отладки при помощи GDB и его основными возможностями.

# 2 Выполнение лабораторной работы

## 2.1 Реализация подпрограмм в NASM

Мы создали каталог для выполнения лабораторной работы №9, перешли в него и добавили файл lab9-1.asm.

В качестве примера рассмотрена программа для вычисления арифметического выражения с использованием подпрограммы calcul. Ввод значения осуществляется с клавиатуры, а вычисление производится в подпрограмме.

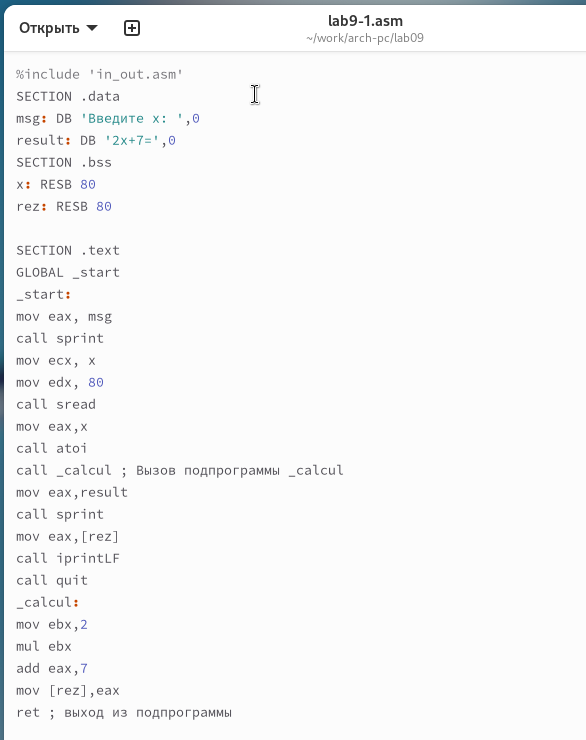


Рис. 1: Программа для вычисления

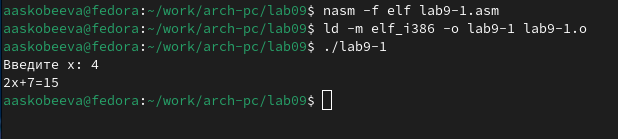


Рис. 2: Результаты выполнения программы для

Изменили текст программы, добавив подпрограмму subcalcul в calcul для вычисления выражения , где , , и вводится с клавиатуры.

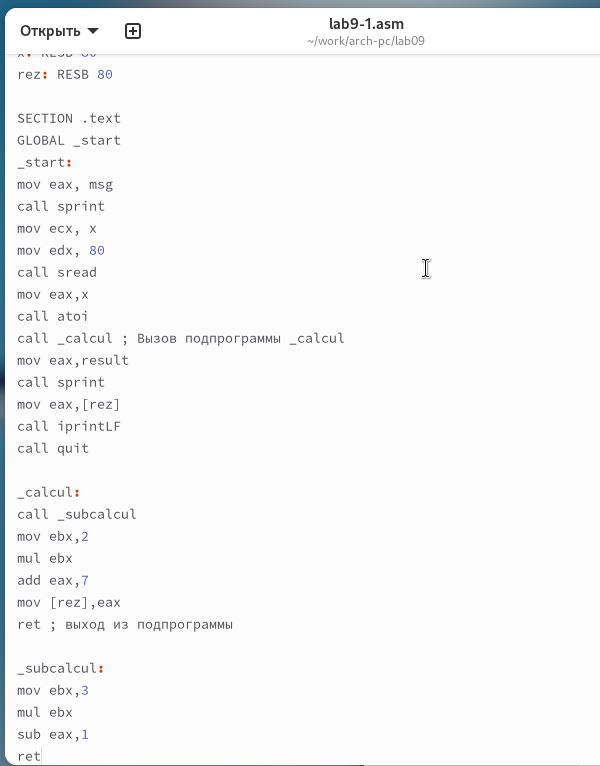


Рис. 3: Программа для вычисления

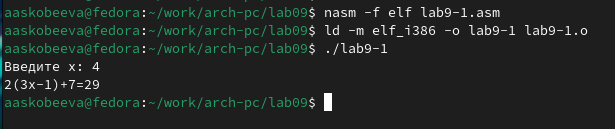


Рис. 4: Результаты выполнения программы для

## 2.2 Отладка программам с помощью GDB

Мы создали файл lab9-2.asm, содержащий текст программы из листинга 9.2 (программа для вывода сообщения “Hello, world!”). Добавили отладочную информацию для работы с GDB, указав флаг -g при трансляции. Программа была протестирована в GDB.



Рис. 5: Программа вывода сообщения “Hello, world!”

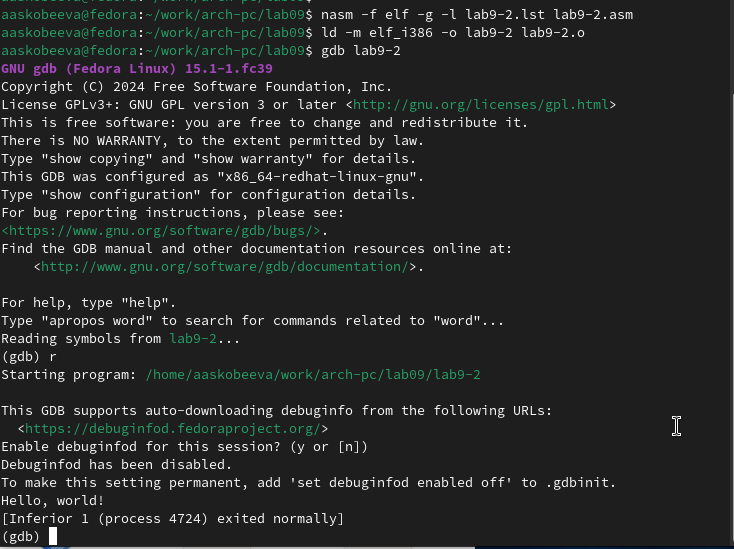


Рис. 6: Запуск программы в GDB

Установили брейкпоинт на метке \_start, запустили программу и просмотрели дизассемблированный код в различных режимах.

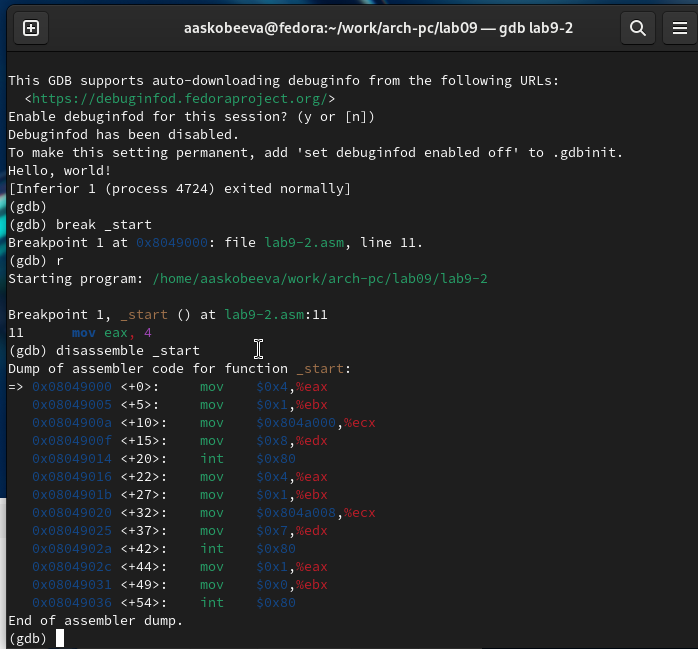


Рис. 7: Дизассемблированный код

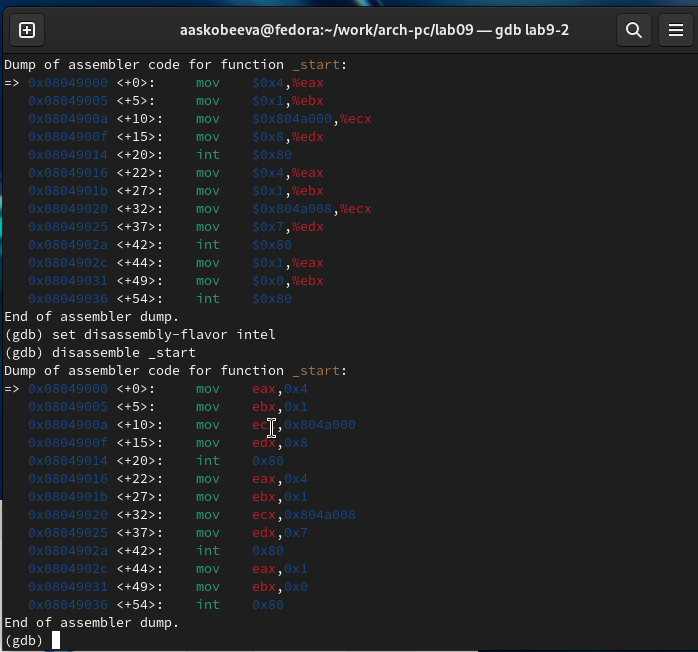


Рис. 8: Дизассемблированный код в режиме Intel

Определили адрес предпоследней инструкции и установили точку останова. Проверили изменения значений регистров с помощью команды stepi.

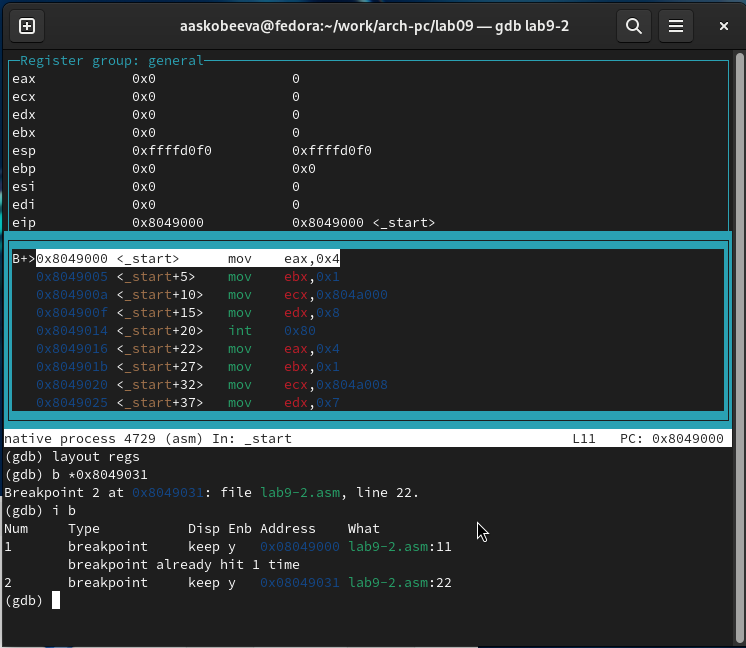


Рис. 9: Установка точки останова

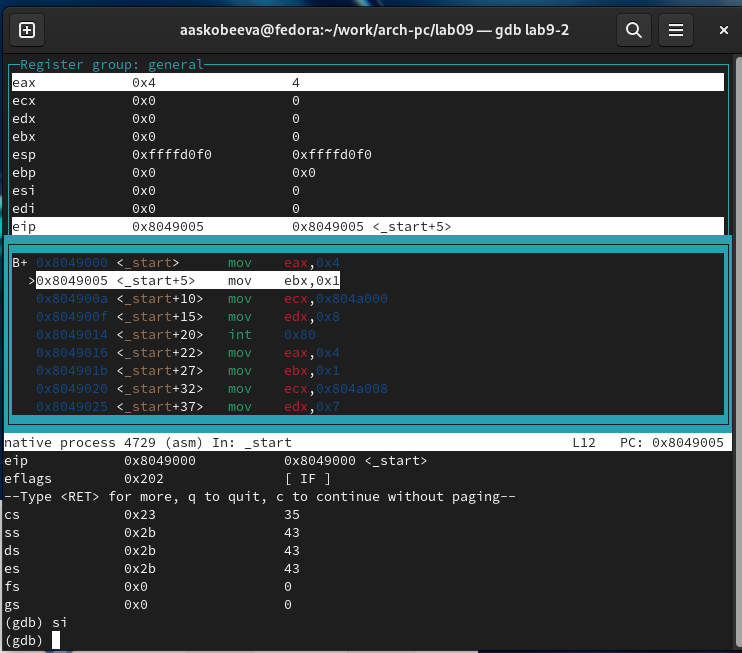


Рис. 10: Просмотр изменений регистров

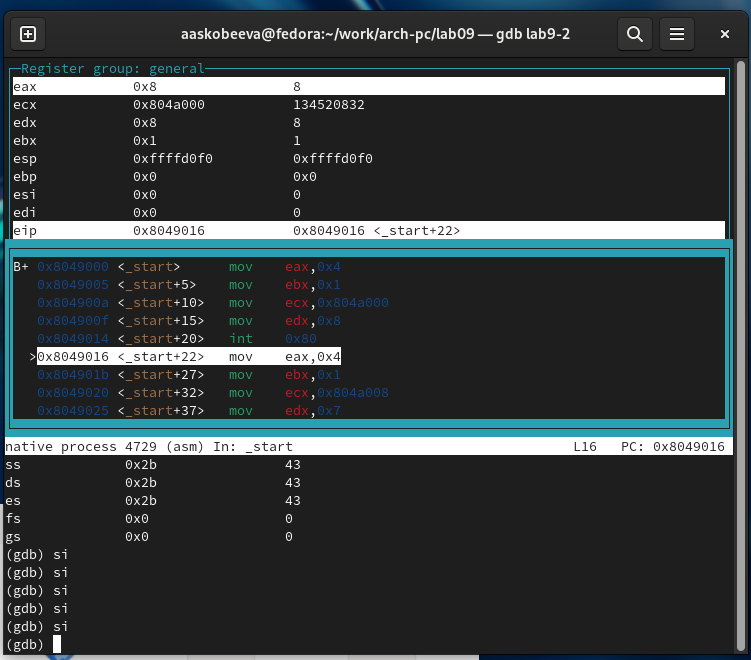


Рис. 11: Дальнейшие изменения регистров

Посмотрели значения переменных msg1 и msg2 по имени и адресу соответственно. Изменили значение первого символа переменной msg1.

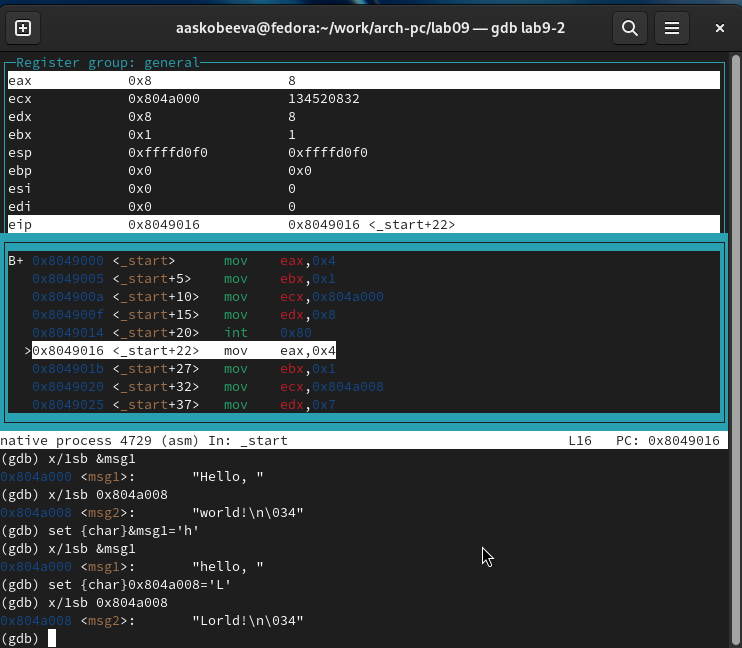


Рис. 12: Изменение значения переменной

Вывели значение регистра edx в различных форматах (шестнадцатеричном, двоичном, символьном) и изменили его значение.

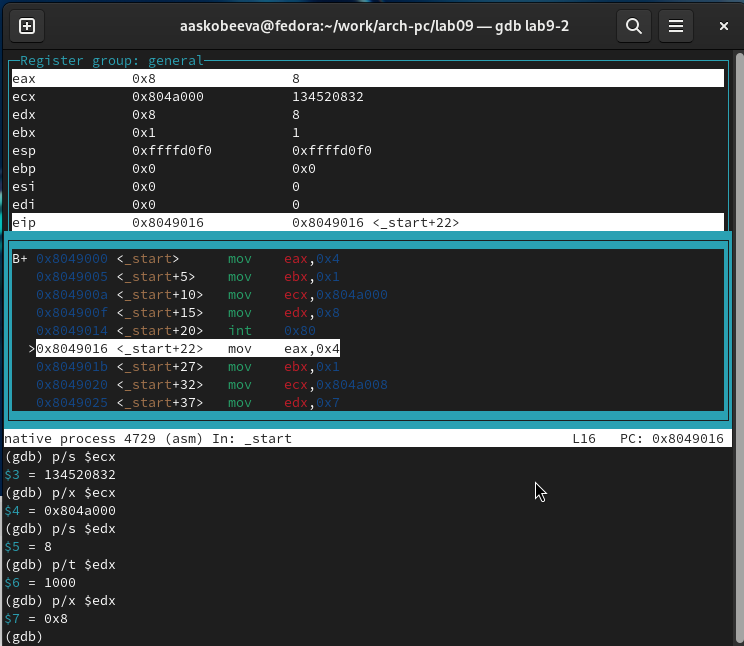


Рис. 13: Вывод значения регистра edx

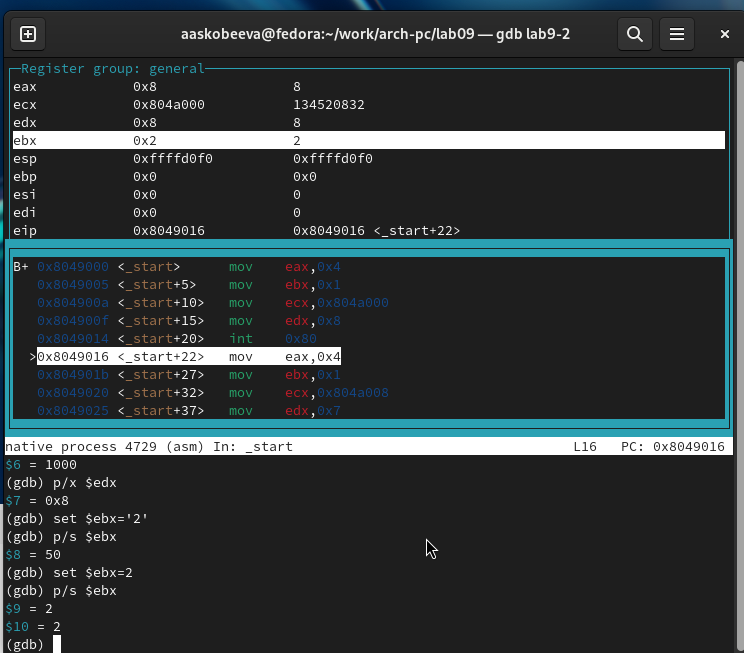


Рис. 14: Изменение регистра ebx

Скопировали файл lab8-2.asm из предыдущей работы, создали исполняемый файл и запустили его с аргументами в GDB, установив точку останова перед началом программы. Исследовали адреса, связанные с аргументами командной строки.

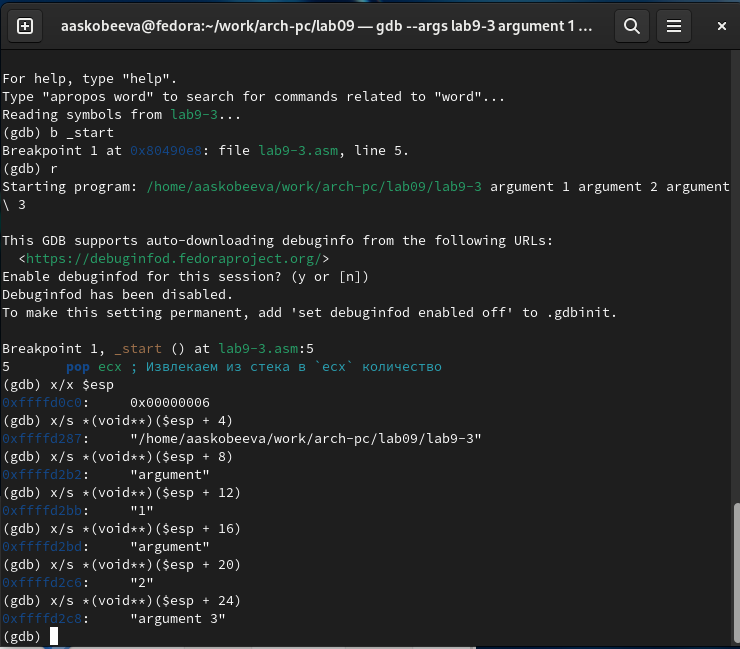


Рис. 15: Исследование стека и аргументов

## 2.3 Задание для самостоятельной работы

Преобразовали программу из лабораторной работы №8 (задание №1) для вычисления значения функции как подпрограмму.

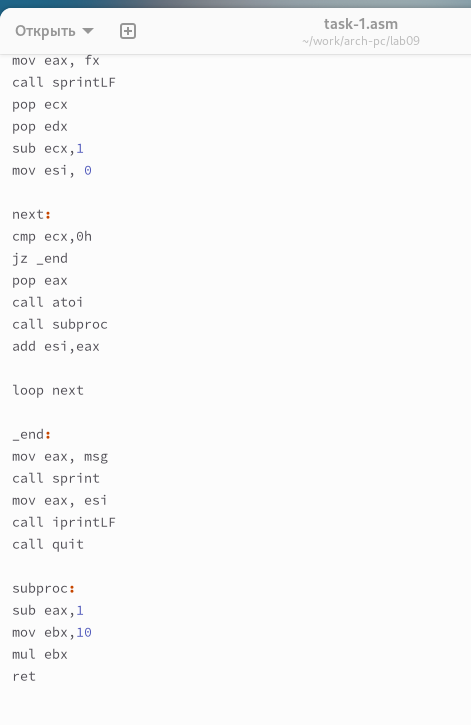


Рис. 16: Программа с подпрограммой для вычисления

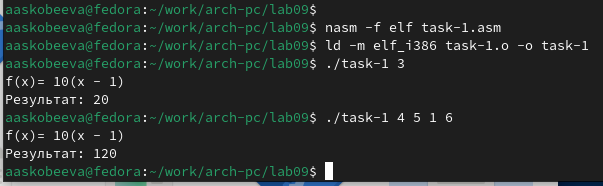


Рис. 17: Результаты выполнения программы

Проанализировали и исправили ошибку в программе для вычисления с помощью отладчика GDB. Ошибка заключалась в неправильном порядке аргументов инструкции add и некорректном завершении программы (использование ebx вместо eax).

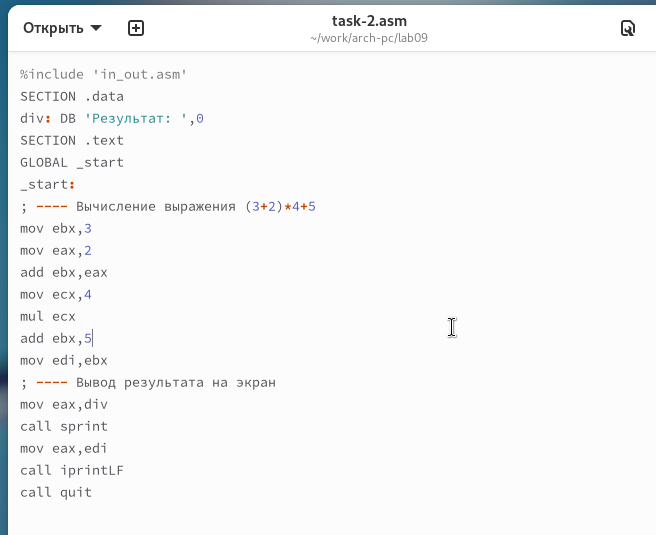


Рис. 18: Код с ошибкой

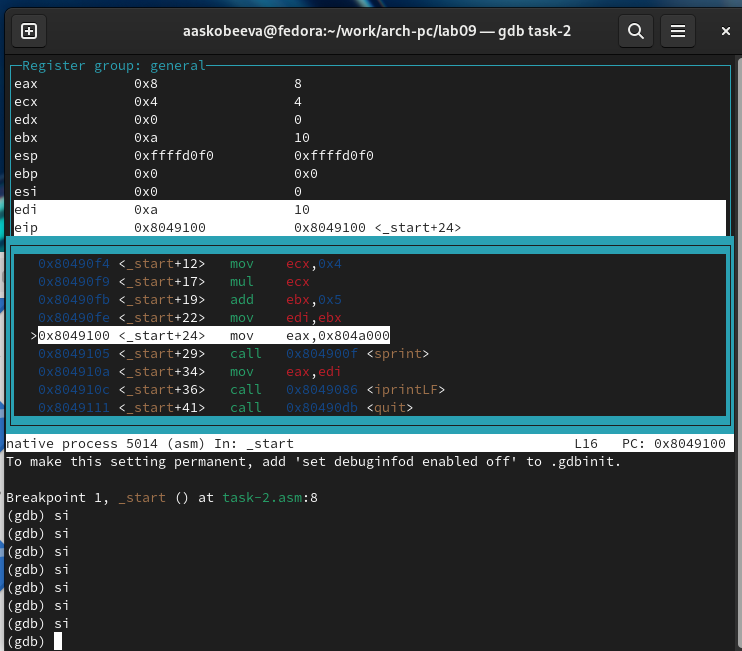


Рис. 19: Процесс отладки

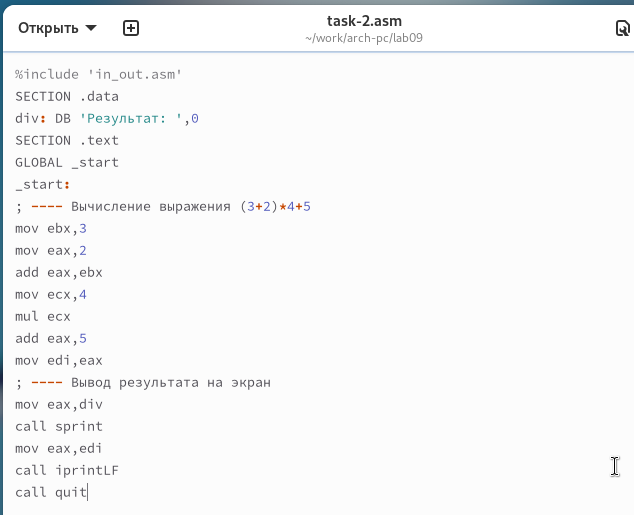


Рис. 20: Исправленный код

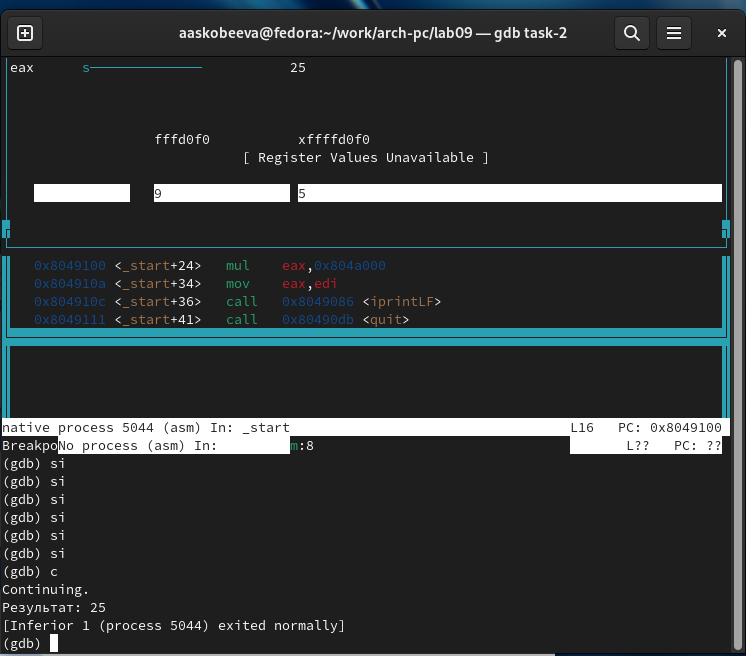


Рис. 21: Проверка исправленного кода

# 3 Выводы

Мы освоили работу с подпрограммами и отладчиком GDB, а также изучили методы анализа и исправления ошибок в ассемблерных программах.