Отчёт по лабораторной работе №9

Цатурьян Лев Вячеславович НММбд-03-23

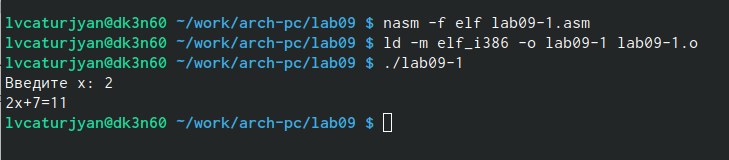
Содержание

# 1 Цель работы

Приобретение навыков использования подпрограмм. Работа с отладчиком

# 2 Выполнение лабораторной работы

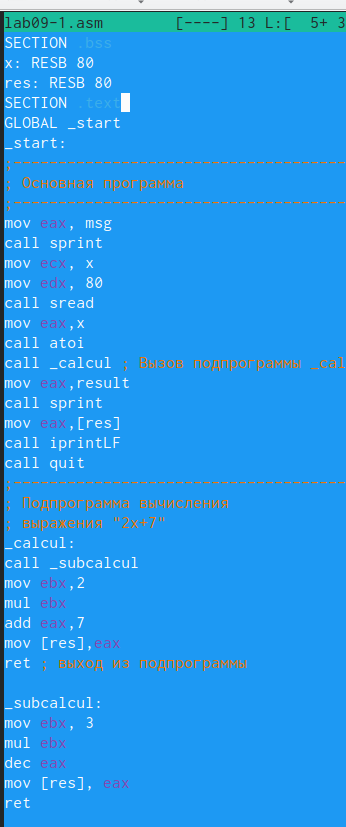
Сначала я создал каталог для программам лабораторной работы № 9, перешёл в него и создал файл lab9-1.asm: Далее я ввёл в созданный файл текст листинга 9.1, создал объектный и исполняемый файлы



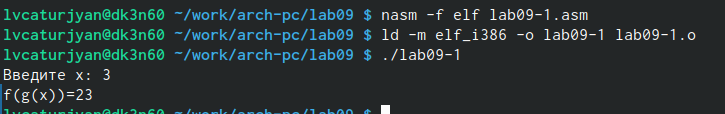
Запуск исполняемого файла

Далее я изменил текст программы добавив подпрограмму subcalcul

Далее я создал объектный и исполняемый файлы и запустил программу



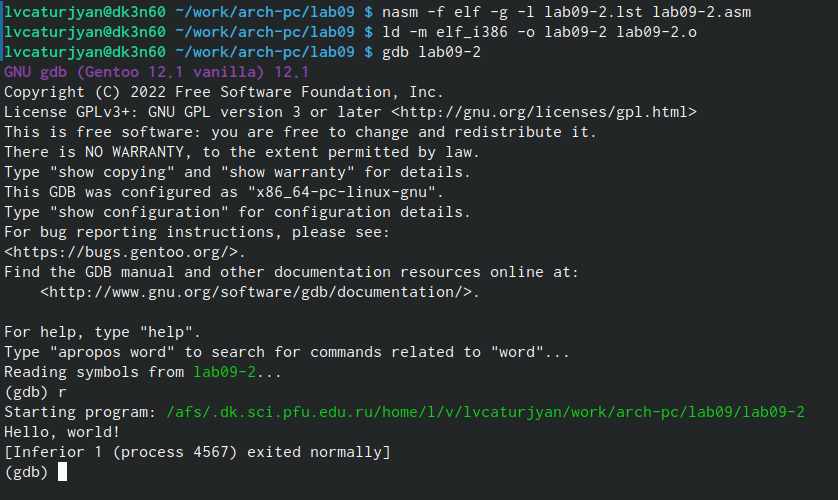
Изменённый текст программы



Создание объектного и исполняемого файлов. Запуск программы

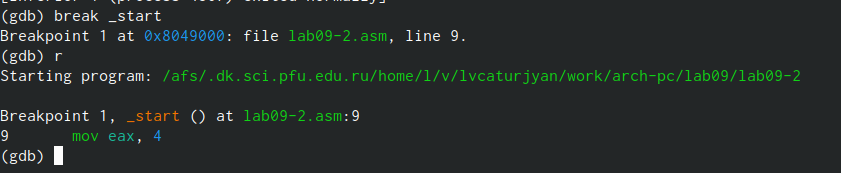
Все работает корректно

Далее я создал файл lab9-2.asm и ввёл в него текст из листинга 9.2 и транслировал этот файл с ключом -g



Запуск отладчика

Я запустил программу с помощью run



Установка брейкпоинта на метку \_start



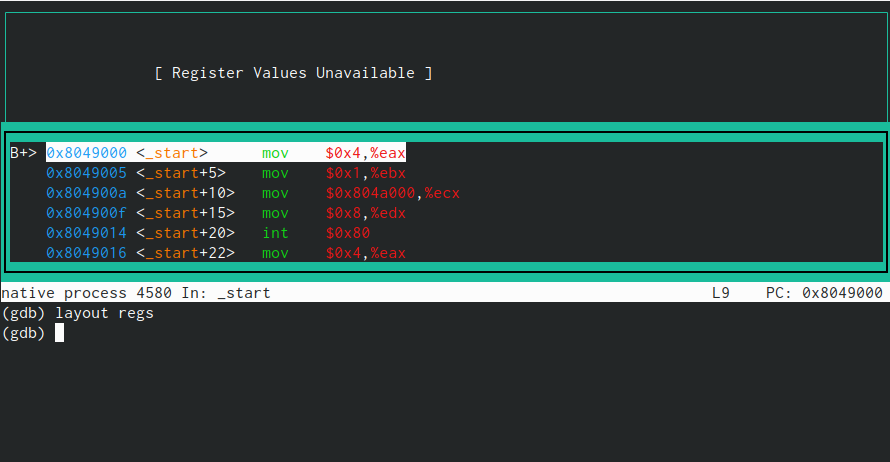
Дисассимилированный код программы с помощью команды disassemble с метки start



Программа с синтаксисом от Intel

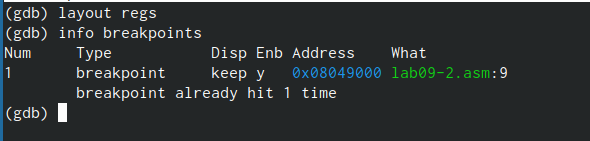
Различия состоят в том, что в дисассимилированном отображении вместо названия регистров пишутся их адреса

Затем я включил режим псевдографики

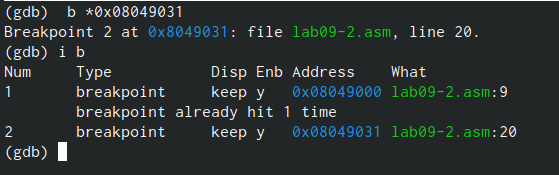


Режим псевдографики

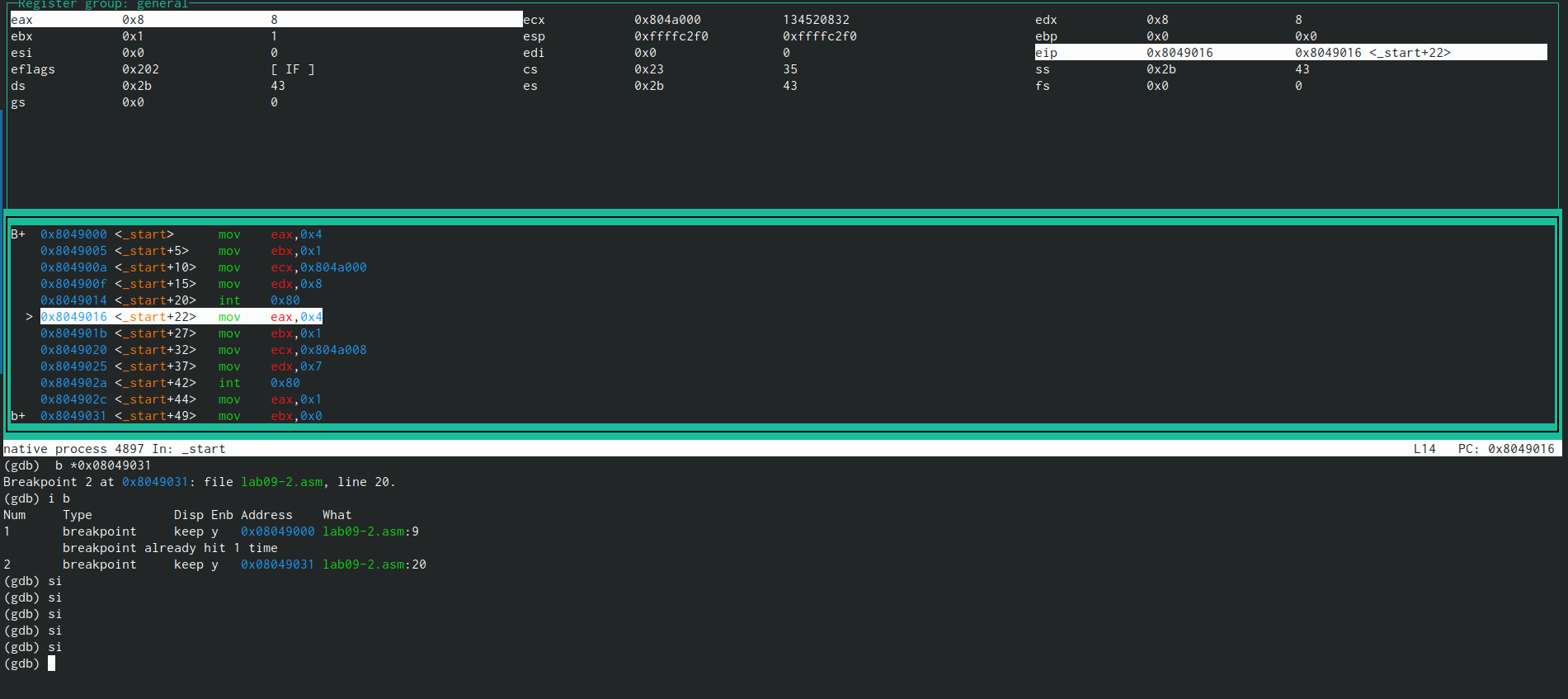
Далее я проверил наличие точек останова в программе с помощью info breakpoints



Точки останова



Установка точки останова по адресу и просмотр информации с помощью i b



5 команд si

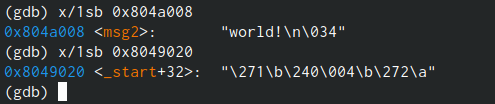
Команда si последовательно выполняет шаги программы, после 5 таких команд изменились значения регистров eax,ebx,ecx,edx

Далее я посмотрел значение переменной msg1 по имени

Просмотр переменной msg1 по имени

Просмотр переменной msg1 по имени

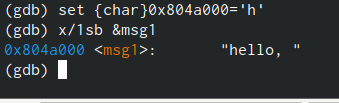
В ней находится слово Hello и знак ,



Просмотр переменной msg2 по адресу

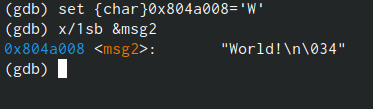
В ней слово world

Далее я изменил букву H на h в msg1

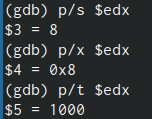


С помощью set меняем значение, выводим на экран

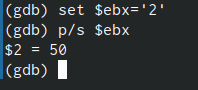
Такую же операцию я проделал с символом w в msg2



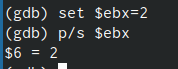
Теперь вместо w стоит W



Вывод значений регистра edx в разных форматах (в шестнадцатеричном, в двоичном и в символьном виде)



Замена значения регистра ebx на ‘2’ и вывод его на экран

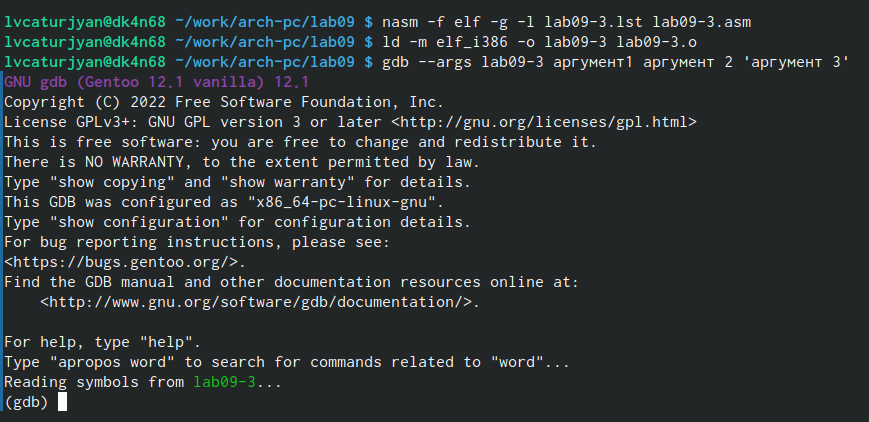


Замена значения регистра ebx на 2 и вывод его на экран

Разница в том, что в первом случае ‘2’ - это символ, а 2 - это число

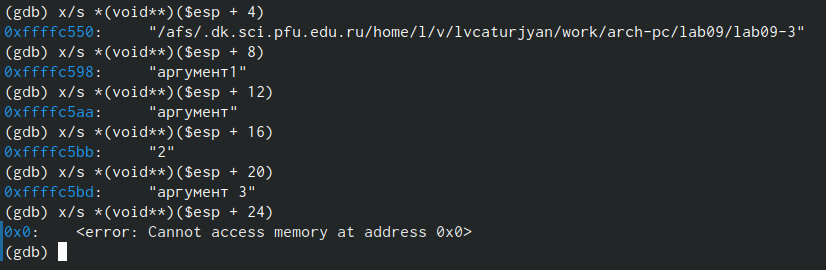
После этого я завершил выполнение программы с помощью с и вышел из отладчика с помощью quit

Далее я скопировал файл lab8-2.asm и назвал его lab9-3.asm, создал и загрузил исполняемый файл в отладчик, указав аргументы



Создание объектного и исполняемого файлов. Запуск программы с заданными аргументами

Далее я задал точку останова перед start и просмотрел позиции стека, в которых находятся аргументы



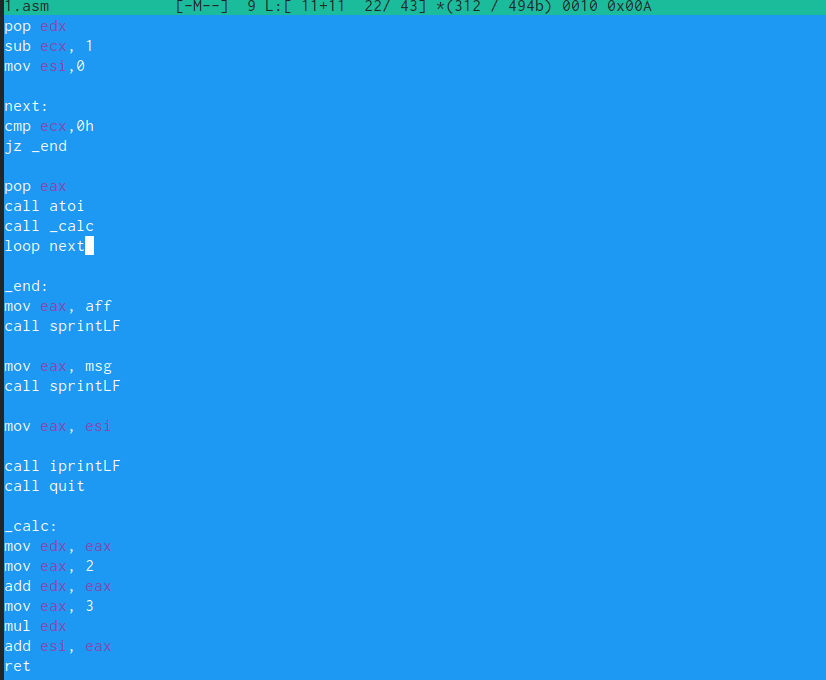
Просмотр позиций стека

Значение меняется на 4, потому что именно на столько байт смещен каждый элемент относительно вершины стека

# 3 Задание для самостоятельной работы

# 4 Задание 1

Это измененная версия программы из лабораторной работы 8, теперь вычисление значения функции 𝑓(𝑥) происходит как подпрограмма



Программа в mc

Её листинг:

%include’in\_out.asm’ ; Цатурьян Лев НММбд-03-23 SECTION .data aff db “Вариант 7. Функция вида y=3(x+2)”,0 msg db “Результат:”,0 SECTION .text global \_start \_start:

pop ecx pop edx sub ecx, 1 mov esi,0

next: cmp ecx,0h jz \_end

pop eax call atoi call \_calc loop next

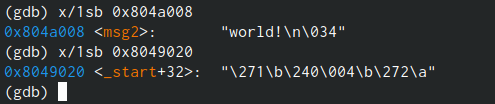
\_end: mov eax, aff call sprintLF

mov eax, msg call sprintLF

mov eax, esi

call iprintLF call quit

\_calc: mov edx, eax mov eax, 2 add edx, eax mov eax, 3 mul edx add esi, eax ret



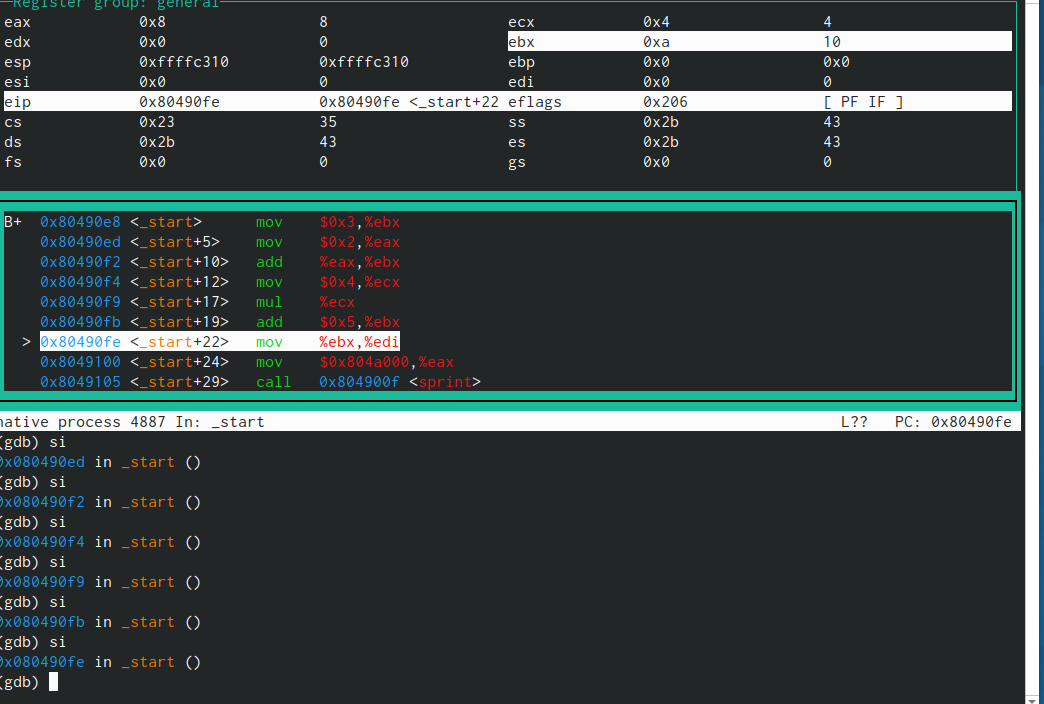
Создание объектного и исполняемого файлов. Запуск программы, работает корректно

# 5 Задание 2

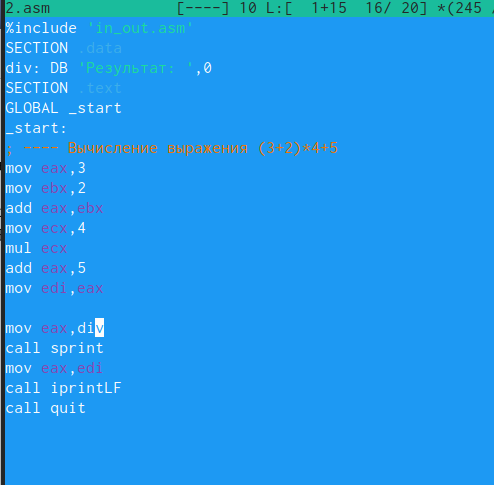
Я открыл программу с помощью отладчика и стал последовательно вводить команды si (выполнение программы по шагам)

Спустя несколько шагов значения, выдаваемые программой и значения вычислений из моей головы перестали совпадать

Я увидел, что результат вычисления выражения (3+2)\*4 записан в регистр eax, после чего к нему нужно прибавить 5,чтобы ответ получился верный, но программа добавляла 5 не к значению регистра eax, а к значению ebx, я исправил эту ошибку



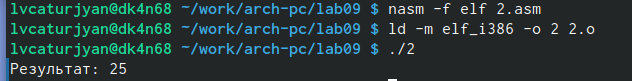
Пошаговое выполнение программы в отладчике



Исправленный текст программы

Текст программы: %include ‘in\_out.asm’ SECTION .data div: DB ‘Результат:’,0 SECTION .text GLOBAL \_start \_start: ; —- Вычисление выражения (3+2)\*4+5 mov eax,3 mov ebx,2 add eax,ebx mov ecx,4 mul ecx add eax,5 mov edi,eax

mov eax,div call sprint mov eax,edi call iprintLF call quit



Работа программы

Программа работает корректно, результаты вычислений были проверены мной вручную

# 6 Выводы

Я приобрёл навыки использования подпрограмм и работы с отладчиком