

Отчёта по лабораторной работе 10

Понятие подпрограммы. Отладчик GDB.

Элина Майзингер НММбд-02-22

Содержание

1	Цель работы	5
2	Задание	6
3	Выполнение лабораторной работы	7
4	Выводы	28

Список иллюстраций

3.1	Файл lab10-1.asm	8
3.2	Работа программы lab10-1.asm	9
3.3	Файл lab10-1.asm	10
3.4	Работа программы lab10-1.asm	11
3.5	Файл lab10-2.asm	12
3.6	Работа программы lab10-2.asm в отладчике	13
3.7	дисассимилированный код	14
3.8	дисассимилированный код в режиме интел	15
3.9	точка остановки	16
3.10	изменение регистров	17
3.11	изменение регистров	18
3.12	изменение значения переменной	19
3.13	вывод значения регистра	20
3.14	вывод значения регистра	21
3.15	вывод значения регистра	22
3.16	Файл lab10-4.asm	23
3.17	Работа программы lab10-4.asm	24
3.18	код с ошибкой	25
3.19	отладка	26
3.20	код исправлен	27
3.21	проверка работы	27

Список таблиц

1 Цель работы

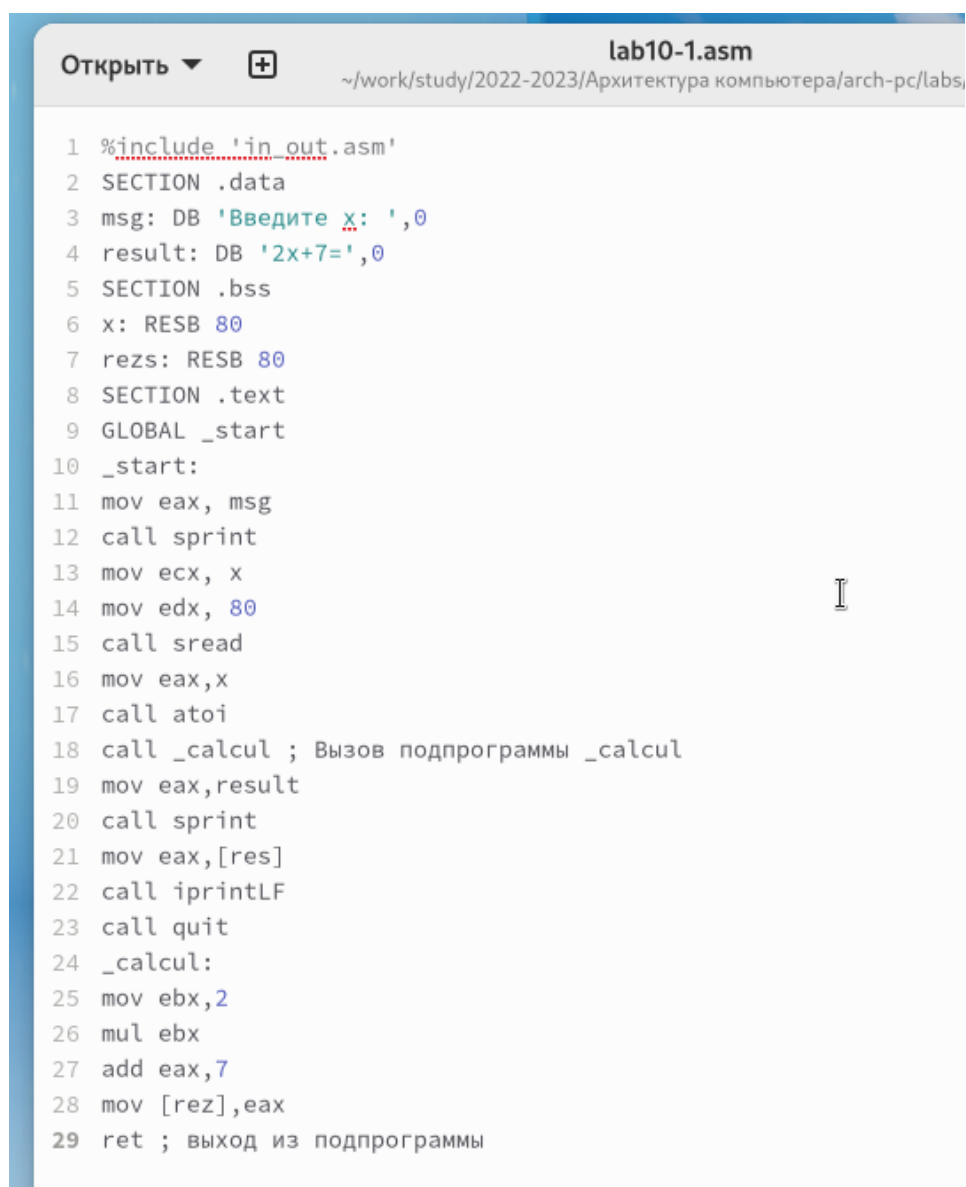
Целью работы является приобретение навыков написания программ с использованием подпрограмм. Знакомство с методами отладки при помощи GDB и его основными возможностями.

2 Задание

1. Изучите примеры реализации подпрограмм
2. Изучите работу с отладчиком GDB
3. Выполните самостоятельное задание
4. Загрузите файлы на GitHub.

3 Выполнение лабораторной работы

1. Создадим каталог для выполнения лабораторной работы № 10, перейдем в него и создадим файл lab10-1.asm:
2. В качестве примера рассмотрим программу вычисления арифметического выражения $f(x) = 2x+7$ с помощью подпрограммы calcul. В данном примере x вводится с клавиатуры, а само выражение вычисляется в подпрограмме. (рис. 3.1, 3.2)



```
1 %include 'in_out.asm'
2 SECTION .data
3 msg: DB 'Введите x: ',0
4 result: DB '2x+7=',0
5 SECTION .bss
6 x: RESB 80
7 rez: RESB 80
8 SECTION .text
9 GLOBAL _start
10 _start:
11 mov eax, msg
12 call sprint
13 mov ecx, x
14 mov edx, 80
15 call sread
16 mov eax, x
17 call atoi
18 call _calcul ; Вызов подпрограммы _calcul
19 mov eax, result
20 call sprint
21 mov eax, [rez]
22 call iprintLF
23 call quit
24 _calcul:
25 mov ebx, 2
26 mul ebx
27 add eax, 7
28 mov [rez], eax
29 ret ; выход из подпрограммы
```

Рис. 3.1: Файл lab10-1.asm


```
[esmayjzinger@fedora lab10]$  
[esmayjzinger@fedora lab10]$  
[esmayjzinger@fedora lab10]$ nasm -f elf lab10-1.asm  
[esmayjzinger@fedora lab10]$ ld -m elf_i386 -o lab10-1 lab10-1.o  
[esmayjzinger@fedora lab10]$ ./lab10-1  
Введите x: 1  
2x+7=9  
[esmayjzinger@fedora lab10]$
```

Рис. 3.2: Работа программы lab10-1.asm

3. Изменим текст программы, добавив подпрограмму subcalcul в подпрограмму calcul, для вычисления выражения $f(g(x))$, где x вводится с клавиатуры, $f(x) = 2x + 7$, $g(x) = 3x - 1$ (рис. 3.3, 3.4)

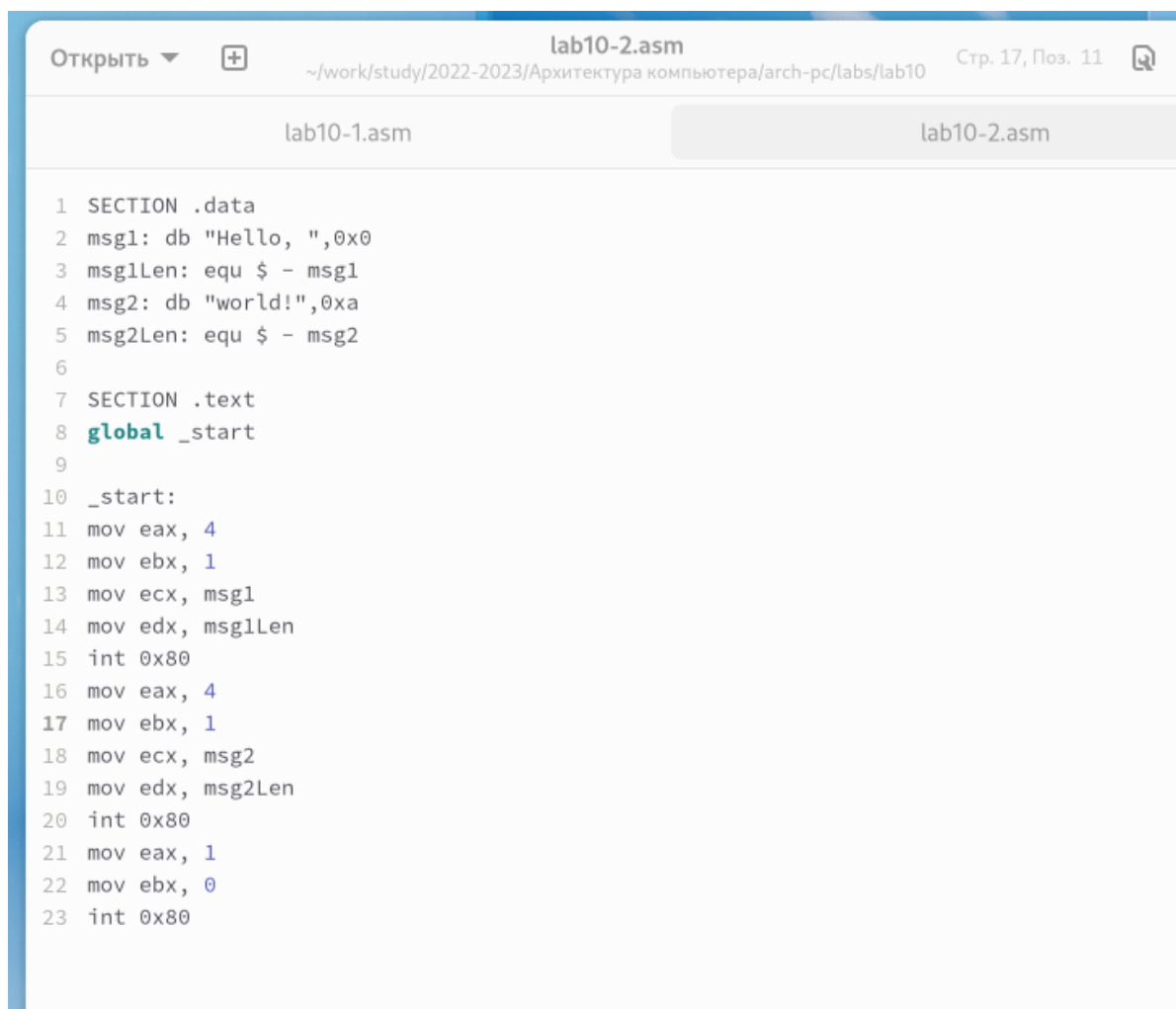
```
9
10 SECTION .text
11 GLOBAL _start
12 _start:
13 mov eax, msg
14 call sprint
15 mov ecx, x
16 mov edx, 80
17 call sread
18 mov eax, x
19 call atoi
20 call _calcul ; Вызов подпрограммы _calcul
21 mov eax, result
22 call sprint
23 mov eax, [rez]
24 call iprintLF
25 call quit
26
27 _calcul:
28 call _subcalcul
29 mov ebx, 2
30 mul ebx
31 add eax, 7
32 mov [rez], eax
33 ret ; выход из подпрограммы
34
35 _subcalcul:
36 mov ebx, 3
37 mul ebx
38 sub eax, 1
39 ret
```

Рис. 3.3: Файл lab10-1.asm

```
[esmayjzinger@fedora lab10]$  
[esmayjzinger@fedora lab10]$  
[esmayjzinger@fedora lab10]$ nasm -f elf lab10-1.asm  
[esmayjzinger@fedora lab10]$ ld -m elf_i386 -o lab10-1 lab10-1.o  
[esmayjzinger@fedora lab10]$ ./lab10-1  
Введите x: 1  
2(3x-1)+7=11  
[esmayjzinger@fedora lab10]$  
[esmayjzinger@fedora lab10]$
```

Рис. 3.4: Работа программы lab10-1.asm

4. Создадим файл lab10-2.asm с текстом программы из Листинга 10.2. (Программа печати сообщения Hello world!): (рис. 3.5)



```
1 SECTION .data
2 msg1: db "Hello, ",0x0
3 msg1Len: equ $ - msg1
4 msg2: db "world!",0xa
5 msg2Len: equ $ - msg2
6
7 SECTION .text
8 global _start
9
10 _start:
11 mov eax, 4
12 mov ebx, 1
13 mov ecx, msg1
14 mov edx, msg1Len
15 int 0x80
16 mov eax, 4
17 mov ebx, 1
18 mov ecx, msg2
19 mov edx, msg2Len
20 int 0x80
21 mov eax, 1
22 mov ebx, 0
23 int 0x80
```

Рис. 3.5: Файл lab10-2.asm

Получим исполняемый файл. Для работы с GDB в исполняемый файл необходимо добавить отладочную информацию, для этого трансляцию программ необходимо проводить с ключом `'-g'`. Затем загрузим исполняемый файл в отладчик gdb: Проверим работу программы, запустив ее в оболочке GDB с помощью команды `run` (сокращённо `r`):(рис. 3.6)

```
This GDB supports auto-downloading debuginfo from the following URLs:
https://debuginfod.fedoraproject.org/
Enable debuginfod for this session? (y or [n])
Debuginfod has been disabled.
To make this setting permanent, add 'set debuginfod enabled off' to .gdbinit.
Hello, world!
[Inferior 1 (process 3189) exited normally]
(gdb) run
Starting program: /home/esmayjzinger/work/study/2022-2023/Архитектура компьютера
/arch-pc/labs/lab10/lab10-2
Hello, world!
[Inferior 1 (process 3198) exited normally]
(gdb) 
```

Рис. 3.6: Работа программы lab10-2.asm в отладчике

Для более подробного анализа программы установим брейкпоинт на метку start, с которой начинается выполнение любой ассемблерной программы, и запустим её. Посмотрим дисассимилированный код программы (рис. 3.7, 3.8)

```
esmayjzinger@fedora:~/work/study/2022-2023/Архитектура к...
Breakpoint 1 at 0x08049000: file lab10-2.asm, line 11.
(gdb) run
Starting program: /home/esmayjzinger/work/study/2022-2023/Архитектура к...
/arch-pc/labs/lab10/lab10-2

Breakpoint 1, _start () at lab10-2.asm:11
11      mov eax, 4
(gdb) disassemble
Dump of assembler code for function _start:
=> 0x08049000 <+0>:      mov     $0x4,%eax
    0x08049005 <+5>:      mov     $0x1,%ebx
    0x0804900a <+10>:     mov     $0x804a000,%ecx
    0x0804900f <+15>:     mov     $0x8,%edx
    0x08049014 <+20>:     int     $0x80
    0x08049016 <+22>:     mov     $0x4,%eax
    0x0804901b <+27>:     mov     $0x1,%ebx
    0x08049020 <+32>:     mov     $0x804a008,%ecx
    0x08049025 <+37>:     mov     $0x7,%edx
    0x0804902a <+42>:     int     $0x80
    0x0804902c <+44>:     mov     $0x1,%eax
    0x08049031 <+49>:     mov     $0x0,%ebx
    0x08049036 <+54>:     int     $0x80
End of assembler dump.
(gdb) 
```

Рис. 3.7: дисассимилированный код

```
End of assembler dump.
(gdb) set disassembly-flavor intel
(gdb) disassemble _start
Dump of assembler code for function _start:
=> 0x08049000 <+0>:      mov     eax,0x4
    0x08049005 <+5>:      mov     ebx,0x1
    0x0804900a <+10>:     mov     ecx,0x804a000
    0x0804900f <+15>:     mov     edx,0x8
    0x08049014 <+20>:     int     0x80
    0x08049016 <+22>:     mov     eax,0x4
    0x0804901b <+27>:     mov     ebx,0x1
    0x08049020 <+32>:     mov     ecx,0x804a008
    0x08049025 <+37>:     mov     edx,0x7
    0x0804902a <+42>:     int     0x80
    0x0804902c <+44>:     mov     eax,0x1
    0x08049031 <+49>:     mov     ebx,0x0
    0x08049036 <+54>:     int     0x80
End of assembler dump.
(gdb)
```

Рис. 3.8: дисассимилированный код в режиме интел

На предыдущих шагах была установлена точка останова по имени метки (`_start`). Проверьте это с помощью команды `info breakpoints` (кратко `i b`) Установим еще одну точку останова по адресу инструкции. Адрес инструкции можно увидеть в средней части экрана в левом столбце соответствующей инструкции. Определим адрес предпоследней инструкции (`mov ebx,0x0`) и установим точку.(рис. 3.9)

```
esmayjzinger@fedora:~/work/study/2022-2023/Архитектура к...

[ Register Values Unavailable ]

B+> 0x8049000 <_start>    mov    eax,0x4
      0x8049005 <_start+5>  mov    ebx,0x1
      0x804900a <_start+10> mov    ecx,0x804a000
      0x804900f <_start+15> mov    edx,0x8
      0x8049014 <_start+20> int     0x80
      0x8049016 <_start+22> mov    eax,0x4
      0x804901b <_start+27> mov    ebx,0x1
      0x8049020 <_start+32> mov    ecx,0x804a008
      0x8049025 <_start+37> mov    edx,0x7
      0x804902a <_start+42> int     0x80

native process 3274 In: _start                                L11
(gdb) layout regs
(gdb)
```

Рис. 3.9: точка остановки

Отладчик может показывать содержимое ячеек памяти и регистров, а при необходимости позволяет вручную изменять значения регистров и переменных. Выполним 5 инструкций с помощью команды `stepi` (или `si`) и проследим за изменением значений регистров. (рис. 3.11 3.12)


```

esmayjzinger@fedora:~/work/study/2022-2023/Архитектура компьютера/arch-pc/labs/lab10 — gdb lab...
Register group: general
eax      0x4      4      ecx      0x0      0
edx      0x0      0      ebx      0x0      0
esp      0xffffd130 0xffffd130  ebp      0x0      0x0
esi      0x0      0      edi      0x0      0
eip      0x8049005 0x8049005 <_start+5>  eflags    0x202     [ IF ]
cs       0x23     35     ss       0x2b     43
ds       0x2b     43     es       0x2b     43
fs       0x0      0      gs       0x0      0

B+ 0x8049000 <_start> mov eax,0x4
> 0x8049005 <_start+5> mov ebx,0x1
0x804900a <_start+10> mov ecx,0x804a000
0x804900f <_start+15> mov edx,0x8
0x8049014 <_start+20> int 0x80
0x8049016 <_start+22> mov eax,0x4
0x804901b <_start+27> mov ebx,0x1
0x8049020 <_start+32> mov ecx,0x804a008
0x8049025 <_start+37> mov edx,0x7
0x804902a <_start+42> int 0x80
0x804902c <_start+44> mov eax,0x1
b+ 0x8049031 <_start+49> mov ebx,0x0

native process 3274 In: _start L12 PC: 0x8049005
ebx      0x0      0
esp      0xffffd130 0xffffd130
ebp      0x0      0x0
esi      0x0      0
edi      0x0      0
eip      0x8049000 0x8049000 <_start>
eflags    0x202     [ IF ]
--Type <RET> for more, q to quit, c to continue without paging--cs      0x23      35
ss       0x2b     43
ds       0x2b     43
es       0x2b     43
fs       0x0      0
gs       0x0      0
(gdb) si
(gdb)

```

Рис. 3.10: изменение регистров

```

esmayjzinger@fedora:~/work/study/2022-2023/Архитектура компьютера/arch-pc/labs/lab10 — gdb lab...
Register group: general
eax      0x8      8      ecx      0x804a000    134520832
edx      0x8      8      ebx      0x1      1
esp      0xffffd130  0xffffd130  ebp      0x0      0x0
esi      0x0      0      edi      0x0      0
eip      0x8049016  0x8049016  <_start+22>  eflags    0x202    [ IF ]
cs       0x23     35      ss       0x2b     43
ds       0x2b     43      es       0x2b     43
fs       0x0      0      gs       0x0      0

B+ 0x8049000 <_start>    mov    eax,0x4
0x8049005 <_start+5>    mov    ebx,0x1
0x804900a <_start+10>   mov    ecx,0x804a000
0x804900f <_start+15>   mov    edx,0x8
0x8049014 <_start+20>   int    0x80
> 0x8049016 <_start+22> mov    eax,0x4
0x804901b <_start+27>   mov    ebx,0x1
0x8049020 <_start+32>   mov    ecx,0x804a008
0x8049025 <_start+37>   mov    edx,0x7
0x804902a <_start+42>   int    0x80
0x804902c <_start+44>   mov    eax,0x1
b+ 0x8049031 <_start+49> mov    ebx,0x0

native process 3274 In: _start L16 PC: 0x8049016
edi      0x0      0
eip      0x8049000  0x8049000 <_start>
eflags    0x202    [ IF ]
--Type <RET> for more, q to quit, c to continue without paging--cs      0x23      35
ss       0x2b     43
ds       0x2b     43
es       0x2b     43
fs       0x0      0
gs       0x0      0
(gdb) si
(gdb) si
(gdb) si
(gdb) si
(gdb) si
(gdb) si

```

Рис. 3.11: изменение регистров

Посмотрим значение переменной msg1 по имени Посмотрим значение переменной msg2 по адресу Изменить значение для регистра или ячейки памяти можно с помощью команды set, задав ей в качестве аргумента имя регистра или адрес. Изменим первый символ переменной msg1 Заменим любой символ во второй переменной msg2. (рис. 3.12)

```

native process 3274 In: _start
(gdb) x/1sb & msg1
0x804a000 <msg1>:      "Hello, "
(gdb) x/1sb 0x804a008
0x804a008 <msg2>:      "world!\n\034"
(gdb) set {char}msg1='h'
'msg1' has unknown type; cast it to its declared type
(gdb) set char&msg1='h'
Argument must be preceded by space.
(gdb) set {char}&msg1='h'
(gdb) x/1sb &msg1
0x804a000 <msg1>:      "hello, "
(gdb) set {char}0x804a008=' '
(gdb) x/1sb 0x804a008
0x804a008 <msg2>:      "Lor!d!\n\034"
(gdb) 

```

Рис. 3.12: изменение значения переменной

Выведем в различных форматах (в шестнадцатеричном формате, в двоичном формате и в символьном виде) значение регистра `edx`. С помощью команды `set` изменим значение регистра `ebx`: (рис. 3.13)

```
native process 3274 In: _start
(gdb) p/s $eax
$1 = 8
(gdb) p/t $eax
$2 = 1000
(gdb) p/s $ecx
$3 = 134520832
(gdb) p/x $ecx
$4 = 0x804a000
(gdb) p/s $edx
$5 = 8
(gdb) p/t $edx
$6 = 1000
(gdb) p/x $edx
$7 = 0x8
(gdb) █
```

Рис. 3.13: вывод значения регистра

С помощью команды set изменим значение регистра ebx:(рис. 3.14)

```
native process 3259 In: _start
```

```
(gdb) p/t $edx
```

```
$6 = 1000
```

```
(gdb) p/x $edx
```

```
$7 = 0x8
```

```
$8 = 0x8
```

```
$9 = 0x8
```

```
$10 = 0x8
```

```
(gdb) set $ebx='2'
```

```
(gdb) p/s $ebx
```

```
$11 = 50
```

```
(gdb) set $ebx=2
```

```
(gdb) p/s $ebx
```

```
$12 = 2
```

```
(gdb) 
```

Рис. 3.14: вывод значения регистра

5. Скопируем файл lab9-2.asm, созданный при выполнении лабораторной работы №9, с программой выводящей на экран аргументы командной строки. Создадим исполняемый файл. Для загрузки в gdb программы с аргументами необходимо использовать ключ `-args`. Загрузим исполняемый файл в отладчик, указав аргументы.

Для начала установим точку останова перед первой инструкцией в программе и запустим ее.

Адрес вершины стека хранится в регистре `esp` и по этому адресу располагается число равное количеству аргументов командной строки (включая имя программы): Как видно, число аргументов равно 5 – это имя программы `lab10-3` и непосредственно аргументы: аргумент1, аргумент, 2 и 'аргумент 3'.

Посмотрим остальные позиции стека – по адресу `[esp+4]` располагается адрес в памяти где находится имя программы, по адресу `[esp+8]` хранится адрес первого аргумента, по адресу `[esp+12]` – второго и т.д. (рис. 3.15)

```
[esmayjzinger@fedora lab10]$
[esmayjzinger@fedora lab10]$ gdb --args lab10-3 argument1 argument1 'argument 3'
GNU gdb (GDB) Fedora 12.1-2.fc36
Copyright (C) 2022 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-redhat-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<https://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
    <http://www.gnu.org/software/gdb/documentation/>.

For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from lab10-3...
(gdb) b _start
Breakpoint 1 at 0x80490e8: file lab10-3.asm, line 5.
(gdb) run
Starting program: /home/esmayjzinger/work/study/2022-2023/Архитектура компьютера
/arch-pc/labs/lab10/lab10-3

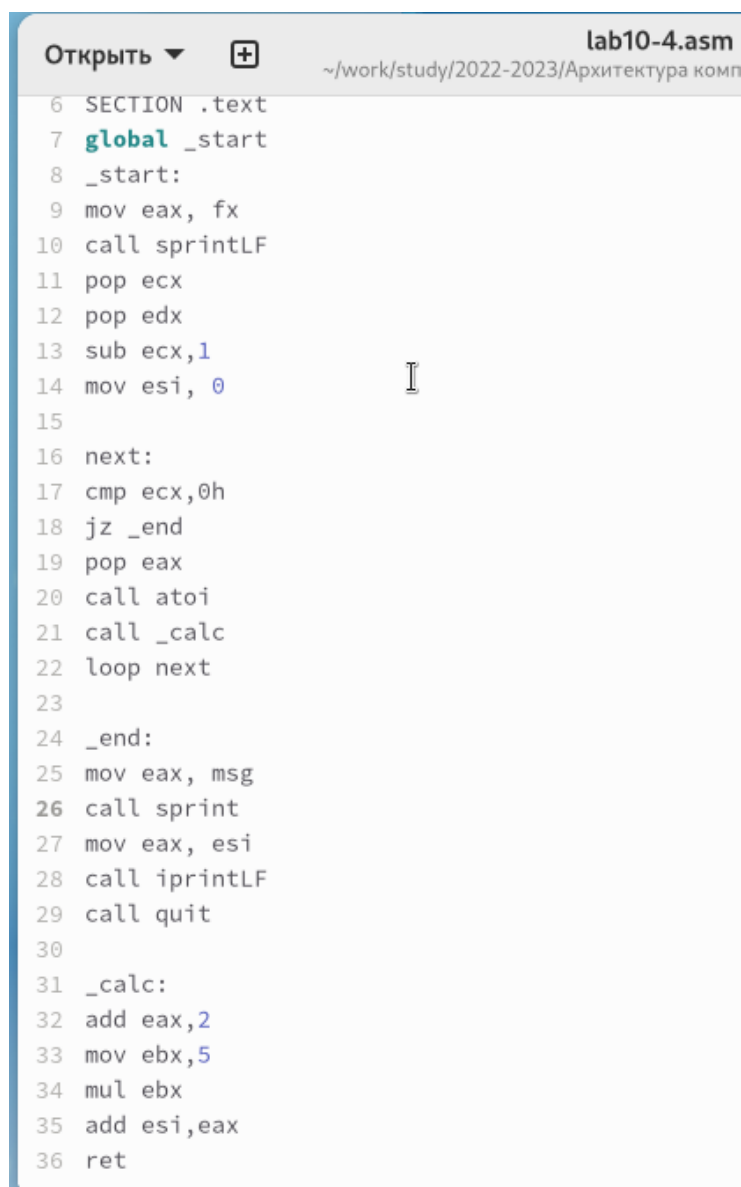
This GDB supports auto-downloading debuginfo from the following URLs:
https://debuginfod.fedoraproject.org/
Enable debuginfod for this session? (y or [n])
Debuginfod has been disabled.
To make this setting permanent, add 'set debuginfod enabled off' to .gdbinit.

Breakpoint 1, _start () at lab10-3.asm:5
5      pop ecx ; Извлекаем из стека в `ecx` количество
(gdb) x/x $esp
0xffffd130:  0x00000001
(gdb)
```

Рис. 3.15: вывод значения регистра

Шаг изменения адреса равен 4, потому что шаг равен размеру переменной - 4 байтам.

6. Преобразуем программу из лабораторной работы №9 (Задание №1 для самостоятельной работы), реализовав вычисление значения функции $f(x)$ как подпрограмму. (рис. 3.16 3.17)



```
lab10-4.asm
~/work/study/2022-2023/Архитектура комп

6 SECTION .text
7 global _start
8 _start:
9 mov eax, fx
10 call sprintLF
11 pop ecx
12 pop edx
13 sub ecx,1
14 mov esi, 0
15
16 next:
17 cmp ecx,0h
18 jz _end
19 pop eax
20 call atoi
21 call _calc
22 loop next
23
24 _end:
25 mov eax, msg
26 call sprint
27 mov eax, esi
28 call iprintLF
29 call quit
30
31 _calc:
32 add eax,2
33 mov ebx,5
34 mul ebx
35 add esi,eax
36 ret
```

Рис. 3.16: Файл lab10-4.asm

```

[esmayjzinger@fedora lab10]$
[esmayjzinger@fedora lab10]$
[esmayjzinger@fedora lab10]$
[esmayjzinger@fedora lab10]$ nasm -f elf lab10-4.asm
[esmayjzinger@fedora lab10]$ ld -m elf_i386 -o lab10-4 lab10-4.o
[esmayjzinger@fedora lab10]$ ./lab10-4 1 2 3 4
f(x)=5(2+x)
Результат: 90
[esmayjzinger@fedora lab10]$
[esmayjzinger@fedora lab10]$
[esmayjzinger@fedora lab10]$ ./lab10-4 1
f(x)=5(2+x)
Результат: 15
[esmayjzinger@fedora lab10]$

```

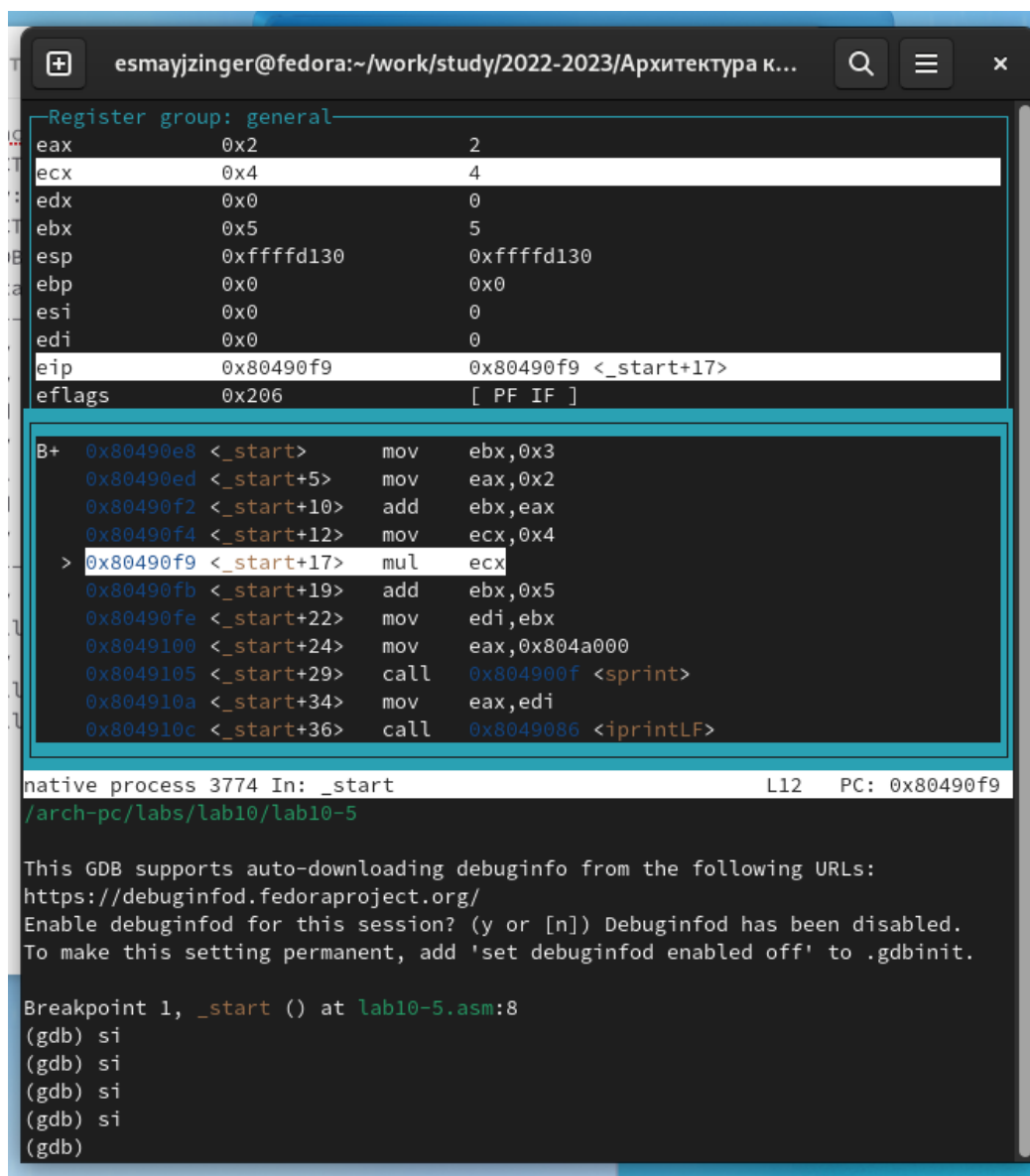
Рис. 3.17: Работа программы lab10-4.asm

7. В листинге приведена программа вычисления выражения $(3+2)*4+5$. При запуске данная программа дает неверный результат. Проверим это. С помощью отладчика GDB, анализируя изменения значений регистров, определим ошибку и исправим ее. (рис. 3.18 3.19 3.20 3.21)


```
Открыть ▾ + lab10-5.asm Стр. 21, Поз. 1
~/work/study/20...ch-pc/labs/lab10

1  %include 'in_out.asm'
2  SECTION .data
3  div: DB 'Результат: ',0
4  SECTION .text
5  GLOBAL _start
6  _start:
7  ; ---- Вычисление выражения (3+2)*4+5
8  mov ebx,3
9  mov eax,2
10 add ebx,eax
11 mov ecx,4
12 mul ecx
13 add ebx,5
14 mov edi,ebx
15 ; ---- Вывод результата на экран
16 mov eax,div
17 call sprint
18 mov eax,edi
19 call iprintLF
20 call quit
21 |
```

Рис. 3.18: код с ошибкой



The screenshot shows a GDB window with the title bar 'esmayjzinger@fedora:~/work/study/2022-2023/Архитектура к...'. The 'Register group: general' section displays the following values:

Register	Value	Comment
eax	0x2	2
ecx	0x4	4
edx	0x0	0
ebx	0x5	5
esp	0xffffd130	0xffffd130
ebp	0x0	0x0
esi	0x0	0
edi	0x0	0
eip	0x80490f9	0x80490f9 <_start+17>
eflags	0x206	[PF IF]

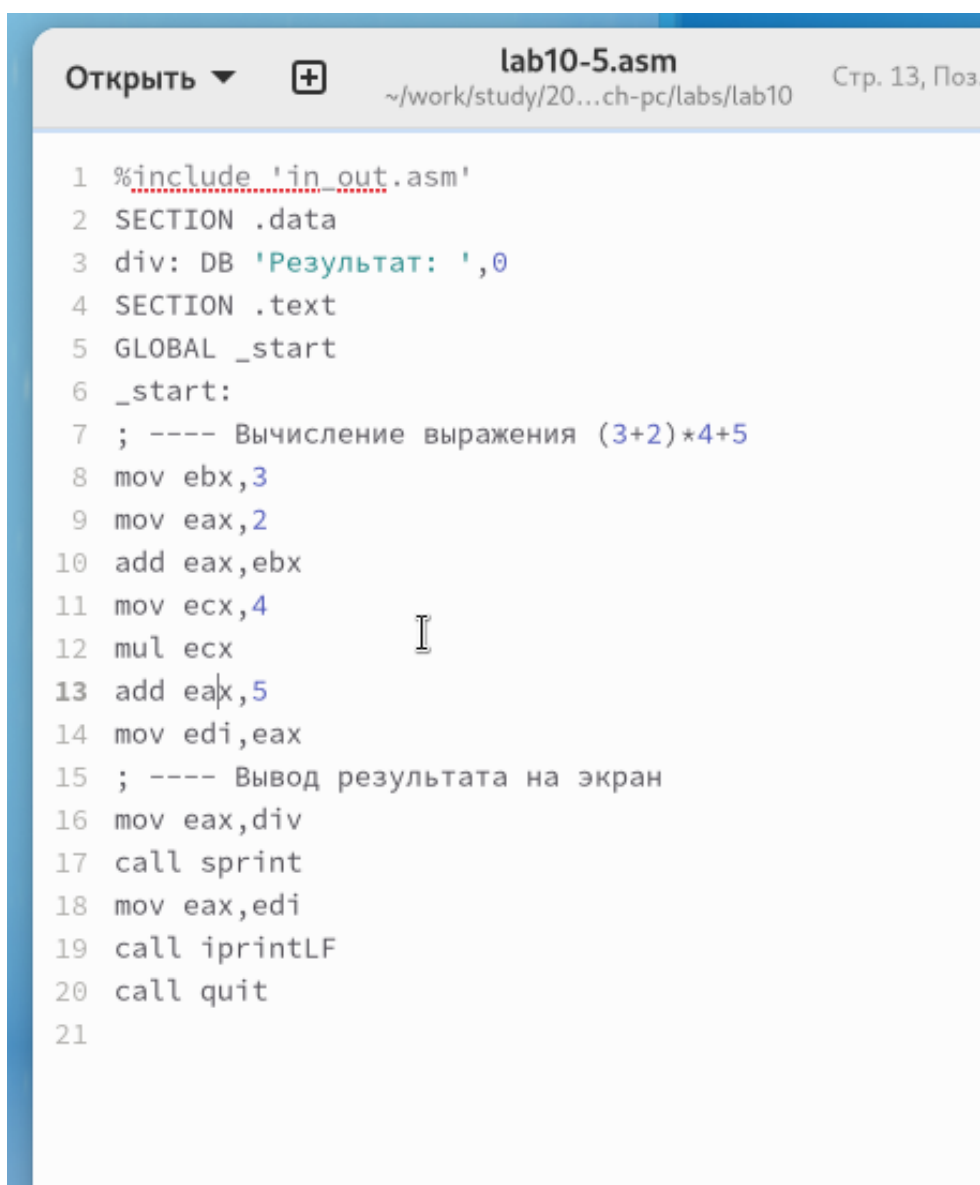
The assembly window shows the following code:

```
B+ 0x80490e8 <_start>    mov     ebx,0x3
0x80490ed <_start+5>    mov     eax,0x2
0x80490f2 <_start+10>   add     ebx,eax
0x80490f4 <_start+12>   mov     ecx,0x4
> 0x80490f9 <_start+17> mul     ecx
0x80490fb <_start+19>   add     ebx,0x5
0x80490fe <_start+22>   mov     edi,ebx
0x8049100 <_start+24>   mov     eax,0x804a000
0x8049105 <_start+29>   call    0x804900f <sprint>
0x804910a <_start+34>   mov     eax,edi
0x804910c <_start+36>   call    0x8049086 <iprintLF>
```

The status bar indicates 'native process 3774 In: _start L12 PC: 0x80490f9'. Below the assembly window, there is a message about debuginfo and a breakpoint set at lab10-5.asm:8.

Рис. 3.19: отладка

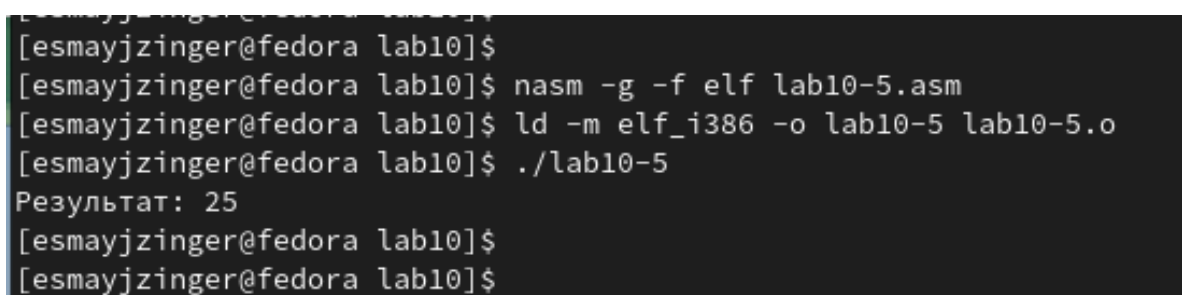
Отметим, что перепутан порядок аргументов у инструкции add и что по окончании работы в edi отправляется ebx вместо eax



```
Открыть ▾ + lab10-5.asm Стр. 13, Поз.
~/work/study/20...ch-pc/labs/lab10

1  %include 'in_out.asm'
2  SECTION .data
3  div: DB 'Результат: ',0
4  SECTION .text
5  GLOBAL _start
6  _start:
7  ; ---- Вычисление выражения (3+2)*4+5
8  mov ebx,3
9  mov eax,2
10 add eax,ebx
11 mov ecx,4
12 mul ecx
13 add eax,5
14 mov edi,eax
15 ; ---- Вывод результата на экран
16 mov eax,div
17 call sprint
18 mov eax,edi
19 call iprintLF
20 call quit
21
```

Рис. 3.20: код исправлен



```
[esmayjzinger@fedora lab10]$
[esmayjzinger@fedora lab10]$ nasm -g -f elf lab10-5.asm
[esmayjzinger@fedora lab10]$ ld -m elf_i386 -o lab10-5 lab10-5.o
[esmayjzinger@fedora lab10]$ ./lab10-5
Результат: 25
[esmayjzinger@fedora lab10]$
[esmayjzinger@fedora lab10]$
```

Рис. 3.21: проверка работы

4 Выводы

Во время выполнения лабораторной работы была освоена работа с подпрограммами и отладчиком.