

Отчёта по лабораторной работе 10

Понятие подпрограммы. Отладчик GDB.

Цвелев С.А. НПИбд-02-22

Содержание

1	Цель работы	5
2	Выполнение лабораторной работы	6
3	Выводы	28

Список иллюстраций

2.1	Файл lab10-1.asm	7
2.2	Работа программы lab10-1.asm	8
2.3	Файл lab10-1.asm	9
2.4	Работа программы lab10-1.asm	10
2.5	Файл lab10-2.asm	11
2.6	Работа программы lab10-2.asm в отладчике	12
2.7	дисассимилированный код	13
2.8	дисассимилированный код в режиме интел	14
2.9	точка остановки	15
2.10	изменение регистров	16
2.11	изменение регистров	17
2.12	изменение значения переменной	18
2.13	вывод значения регистра	19
2.14	вывод значения регистра	20
2.15	вывод значения регистра	22
2.16	Файл lab10-4.asm	23
2.17	Работа программы lab10-4.asm	23
2.18	код с ошибкой	24
2.19	отладка	25
2.20	код исправлен	26
2.21	проверка работы	27

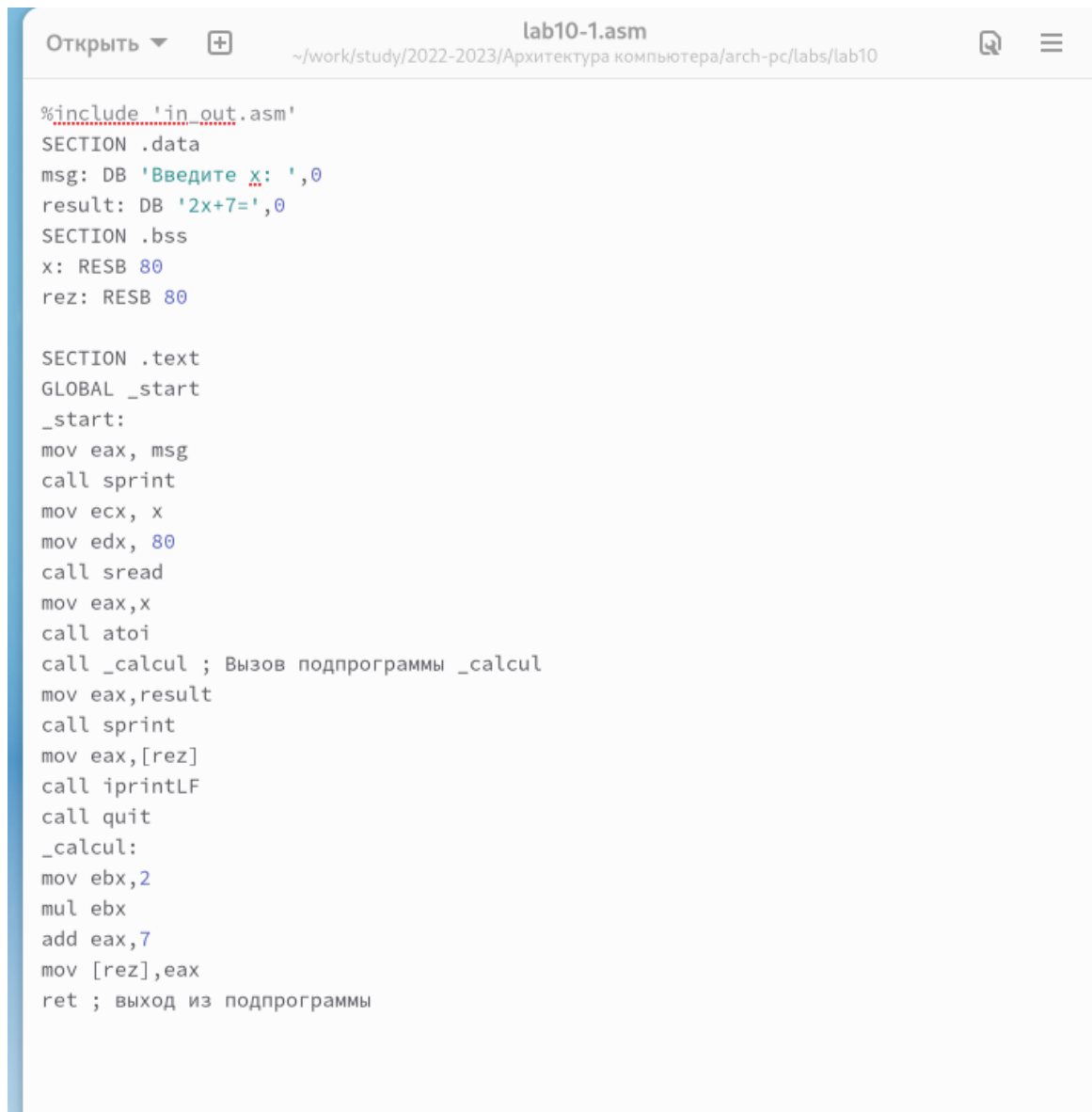
Список таблиц

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 Выполнение лабораторной работы

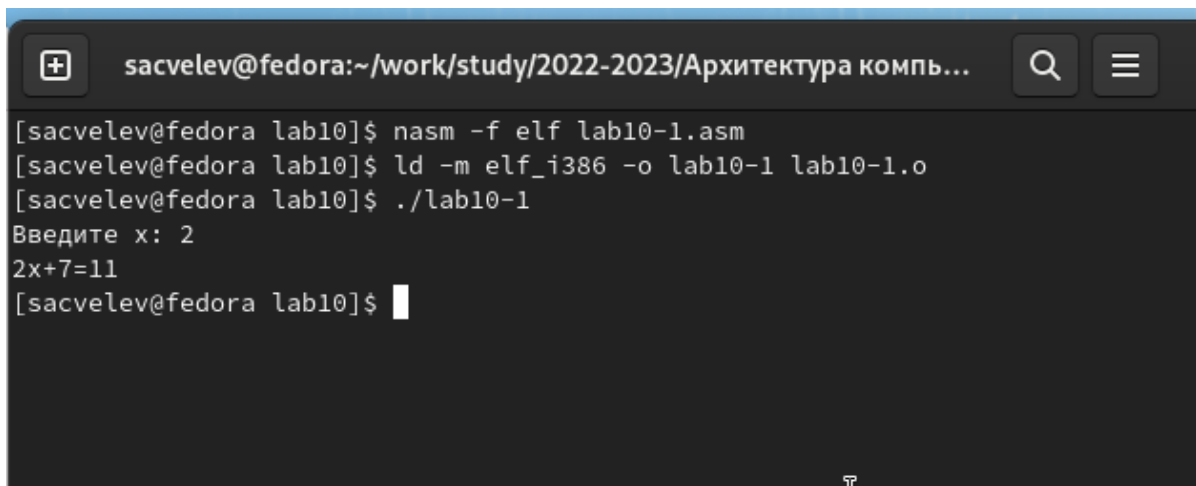
1. Создайте каталог для выполнения лабораторной работы № 10, перейдите в него и создайте файл lab10-1.asm:
2. В качестве примера рассмотрим программу вычисления арифметического выражения $f(x) = 2x+7$ с помощью подпрограммы calcul. В данном примере x вводится с клавиатуры, а само выражение вычисляется в подпрограмме. Внимательно изучите текст программы (Листинг 10.1). (рис. 2.1, 2.2)



```
%include 'in_out.asm'
SECTION .data
msg: DB 'Введите x: ',0
result: DB '2x+7=',0
SECTION .bss
x: RESB 80
rez: RESB 80

SECTION .text
GLOBAL _start
_start:
mov eax, msg
call sprint
mov ecx, x
mov edx, 80
call sread
mov eax, x
call atoi
call _calcul ; Вызов подпрограммы _calcul
mov eax, result
call sprint
mov eax, [rez]
call iprintLF
call quit
_calcul:
mov ebx, 2
mul ebx
add eax, 7
mov [rez], eax
ret ; выход из подпрограммы
```

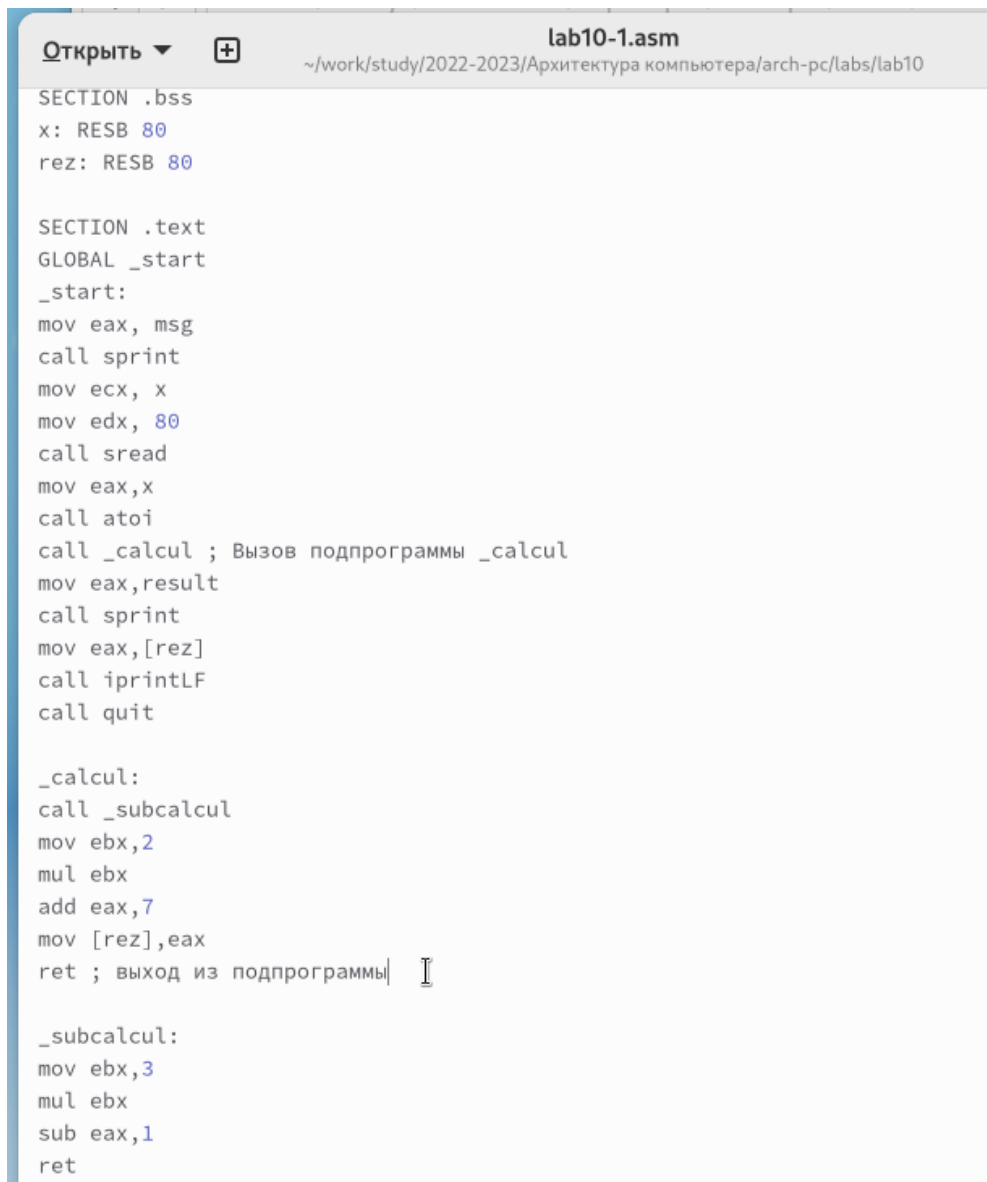
Рис. 2.1: Файл lab10-1.asm



```
sacvelev@fedora:~/work/study/2022-2023/Архитектура компь...  
[sacvelev@fedora lab10]$ nasm -f elf lab10-1.asm  
[sacvelev@fedora lab10]$ ld -m elf_i386 -o lab10-1 lab10-1.o  
[sacvelev@fedora lab10]$ ./lab10-1  
Введите x: 2  
2x+7=11  
[sacvelev@fedora lab10]$
```

Рис. 2.2: Работа программы lab10-1.asm

3. Измените 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. 2.3, 2.4)



```
lab10-1.asm
~/work/study/2022-2023/Архитектура компьютера/arch-пс/labs/lab10

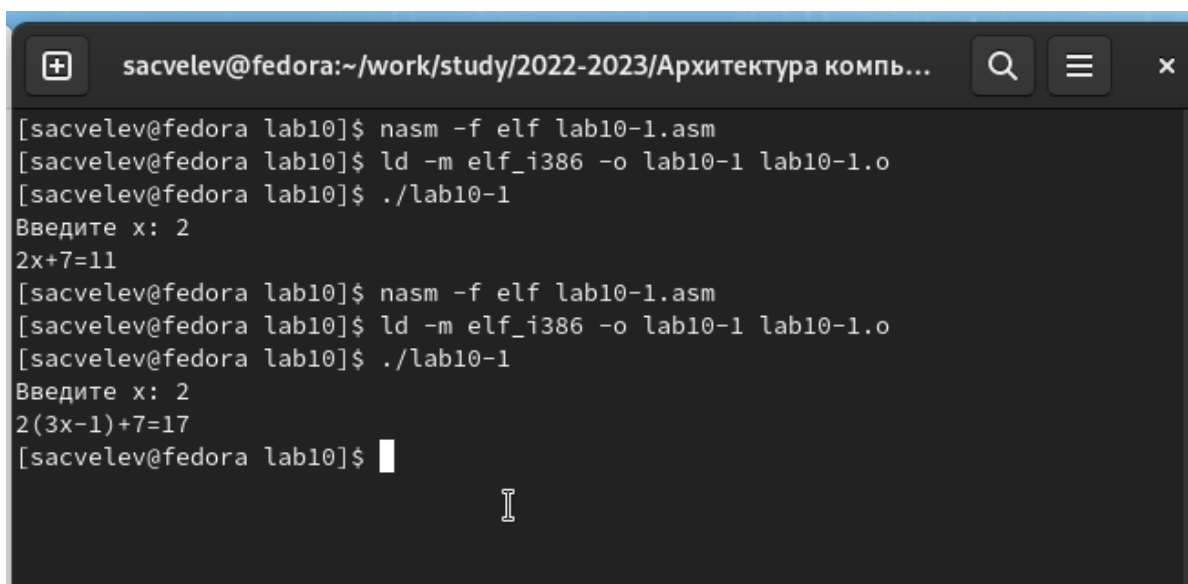
SECTION .bss
x: RESB 80
rez: RESB 80

SECTION .text
GLOBAL _start
_start:
mov eax, msg
call sprint
mov ecx, x
mov edx, 80
call sread
mov eax, x
call atoi
call _calcul ; Вызов подпрограммы _calcul
mov eax, result
call sprint
mov eax, [rez]
call iprintLF
call quit

_calcul:
call _subcalcul
mov ebx, 2
mul ebx
add eax, 7
mov [rez], eax
ret ; выход из подпрограммы

_subcalcul:
mov ebx, 3
mul ebx
sub eax, 1
ret
```

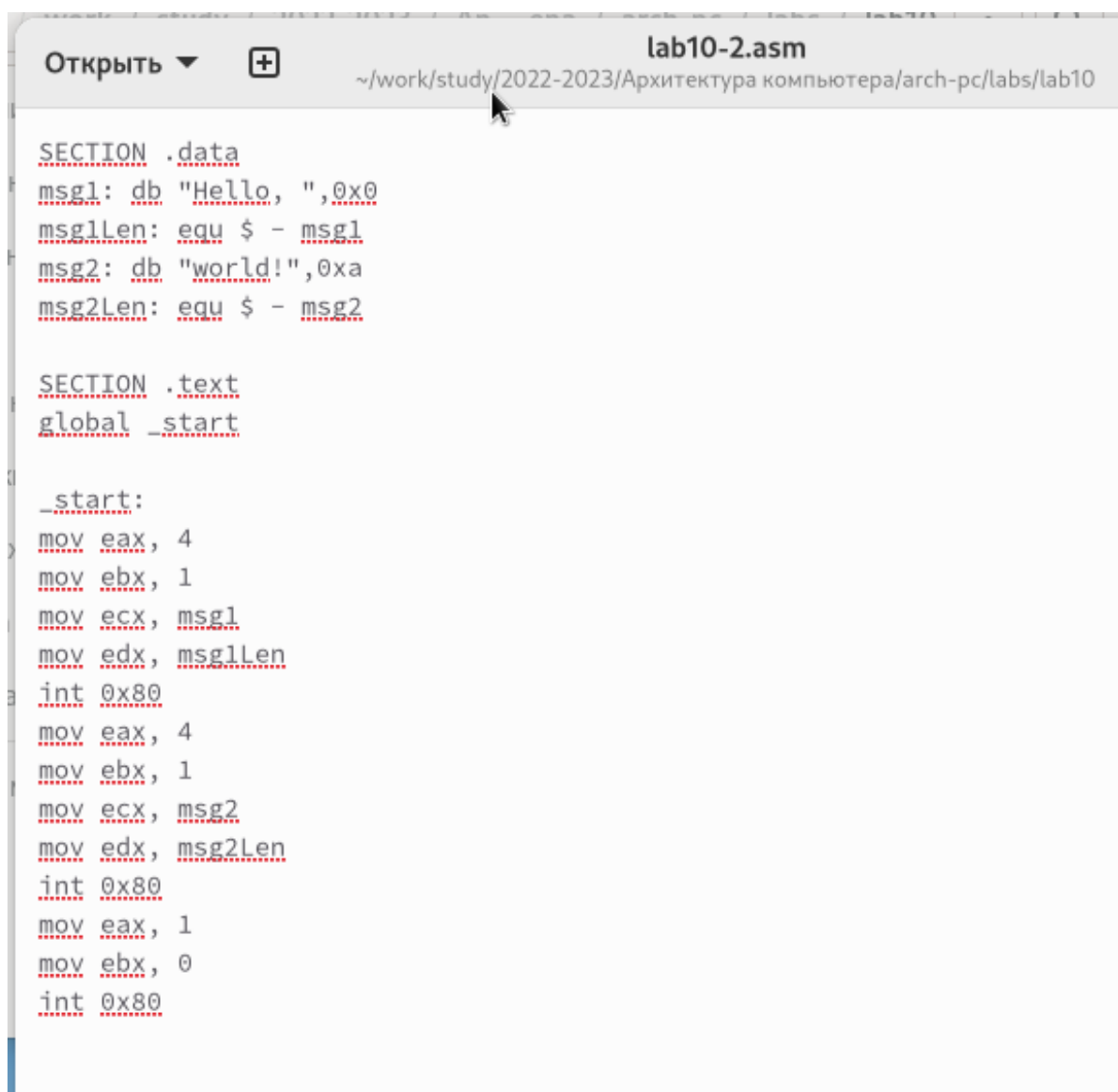
Рис. 2.3: Файл lab10-1.asm



```
sacvelev@fedora:~/work/study/2022-2023/Архитектура компь...
[sacvelev@fedora lab10]$ nasm -f elf lab10-1.asm
[sacvelev@fedora lab10]$ ld -m elf_i386 -o lab10-1 lab10-1.o
[sacvelev@fedora lab10]$ ./lab10-1
Введите x: 2
2x+7=11
[sacvelev@fedora lab10]$ nasm -f elf lab10-1.asm
[sacvelev@fedora lab10]$ ld -m elf_i386 -o lab10-1 lab10-1.o
[sacvelev@fedora lab10]$ ./lab10-1
Введите x: 2
2(3x-1)+7=17
[sacvelev@fedora lab10]$
```

Рис. 2.4: Работа программы lab10-1.asm

4. Создайте файл lab10-2.asm с текстом программы из Листинга 10.2. (Программа печати сообщения Hello world!); (рис. 2.5)



```
lab10-2.asm
~/work/study/2022-2023/Архитектура компьютера/arch-pc/labs/lab10

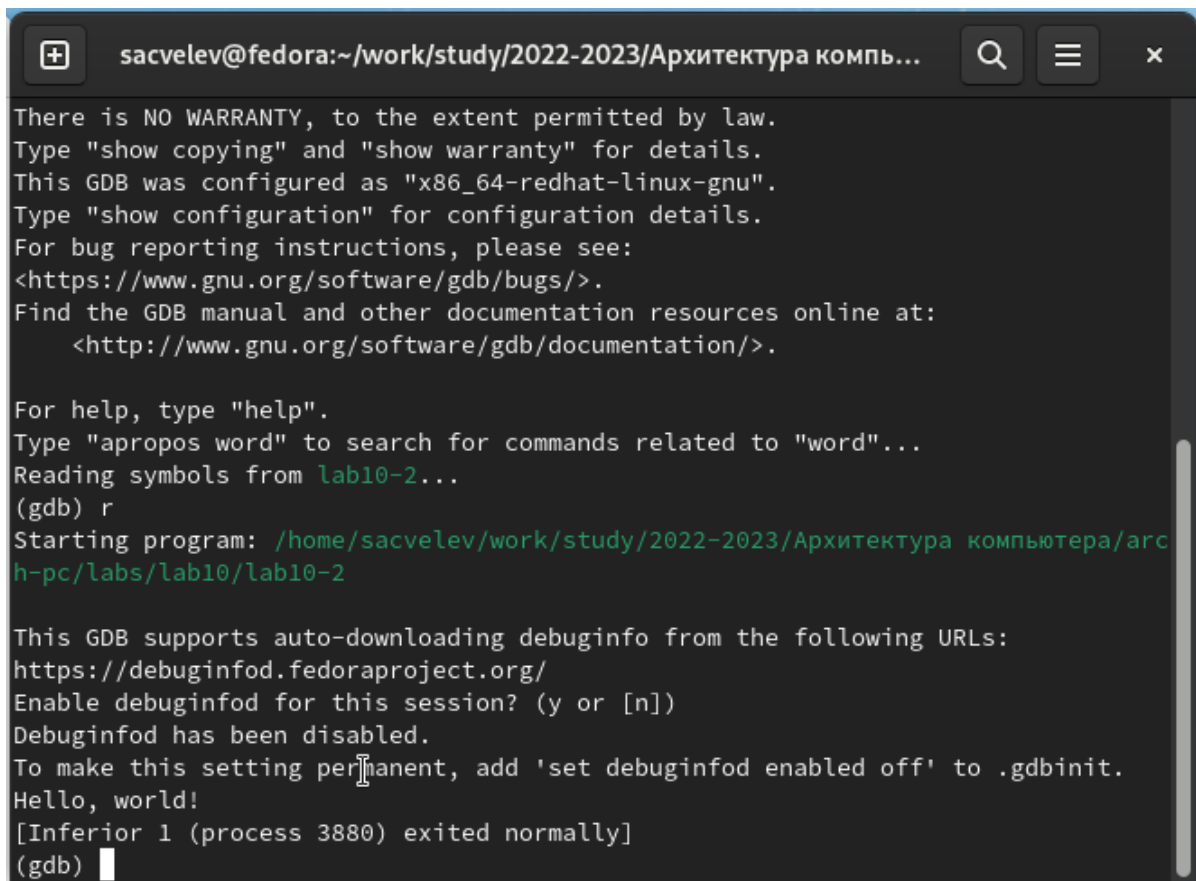
SECTION .data
msg1: db "Hello, ",0x0
msg1len: equ $ - msg1
msg2: db "world!",0xa
msg2len: equ $ - msg2

SECTION .text
global _start

_start:
mov eax, 4
mov ebx, 1
mov ecx, msg1
mov edx, msg1len
int 0x80
mov eax, 4
mov ebx, 1
mov ecx, msg2
mov edx, msg2len
int 0x80
mov eax, 1
mov ebx, 0
int 0x80
```

Рис. 2.5: Файл lab10-2.asm

Получите исполняемый файл. Для работы с GDB в исполняемый файл необходимо добавить отладочную информацию, для этого трансляцию программ необходимо проводить с ключом '-g'. Загрузите исполняемый файл в отладчик gdb: Проверьте работу программы, запустив ее в оболочке GDB с помощью команды run (сокращённо r):(рис. 2.6)



The screenshot shows a terminal window with the title bar "sacvelev@fedora:~/work/study/2022-2023/Архитектура компь...". The terminal output is as follows:

```
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 lab10-2...
(gdb) r
Starting program: /home/sacvelev/work/study/2022-2023/Архитектура компьютера/arc
h-pc/labs/lab10/lab10-2

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 3880) exited normally]
(gdb) 
```

Рис. 2.6: Работа программы lab10-2.asm в отладчике

Для более подробного анализа программы установите брейкпоинт на метку start, с которой начинается выполнение любой ассемблерной программы, и запустите её. Посмотрите дисассимилированный код программы (рис. 2.7, 2.8)

```

sacvelev@fedora:~/work/study/2022-2023/Архитектура компь...
Breakpoint 1 at 0x8049000: file lab10-2.asm, line 11.
(gdb) r
Starting program: /home/sacvelev/work/study/2022-2023/Архитектура компь...
h-pc/labs/lab10/lab10-2

Breakpoint 1, _start () at lab10-2.asm:11
11      mov eax, 4
(gdb) disassemble _start
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. 2.7: дисассимилированный код

```
sacvelev@fedora:~/work/study/2022-2023/Архитектура компь...

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) 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. 2.8: 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. Определите адрес предпоследней инструкции (`mov ebx,0x0`) и установите точку.(рис. 2.9)

```
sacvelev@fedora:~/work/study/2022-2023/Архитектура компь...
Register group: general
eax      0x4      4
ecx      0x0      0
edx      0x0      0
ebx      0x0      0
esp      0xffffd160 0xffffd160
ebp      0x0      0x0
esi      0x0      0
edi      0x0      0
eip      0x8049005 0x8049005 <_start+5>
eflags   0x202    [ IF ]

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

native process 3900 In: _start L12 PC: 0x8049005
edi      0x0      0
eip      0x8049000 0x8049000 <_start>
eflags   0x202    [ IF ]
cs       0x23     35
--Type <RET> for more, q to quit, c to continue without paging-- 0
x2b      43
ds       0x2b     43
es       0x2b     43
fs       0x0      0
gs       0x0      0
(gdb) si
(gdb) 
```

Рис. 2.9: точка остановки

Отладчик может показывать содержимое ячеек памяти и регистров, а при необходимости позволяет вручную изменять значения регистров и переменных. Выполните 5 инструкций с помощью команды `stepi` (или `si`) и проследите за изменением значений регистров. (рис. 2.11 2.12)

```
sacvelev@fedora:~/work/study/2022-2023/Архитектура компь...
Register group: general
eax      0x4      4
ecx      0x0      0
edx      0x0      0
ebx      0x0      0
esp      0xffffd160 0xffffd160
ebp      0x0      0x0
esi      0x0      0
edi      0x0      0
eip      0x8049005 0x8049005 <_start+5>
eflags   0x202    [ IF ]

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

native process 3900 In: _start L12 PC: 0x8049005
edi      0x0      0
eip      0x8049000 0x8049000 <_start>
eflags   0x202    [ IF ]
cs       0x23     35
--Type <RET> for more, q to quit, c to continue without paging--ss 0
x2b      43
ds       0x2b     43
es       0x2b     43
fs       0x0      0
gs       0x0      0
(gdb) si
(gdb) 
```

Рис. 2.10: изменение регистров


```
sacvelev@fedora:~/work/study/2022-2023/Архитектура компь...
Register group: general
eax      0x4      4
ecx      0x804a008 134520840
edx      0x7      7
ebx      0x1      1
esp      0xffffd160 0xffffd160
ebp      0x0      0x0
esi      0x0      0
edi      0x0      0
eip      0x804902a 0x804902a <_start+42>
eflags   0x202    [ IF ]

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
0x8049036 <_start+54> int 0x80
0x8049038      add BYTE PTR [eax],al
0x804903a      add BYTE PTR [eax],al

native process 3900 In: _start L20 PC: 0x804902a
fs      0x0      0
gs      0x0      0
(gdb) si
(gdb) si
(gdb) si
(gdb) si
(gdb) si
(gdb) si
(gdb) si
(gdb) si
(gdb) si
(gdb) si
(gdb) si
```

Рис. 2.11: изменение регистров

Посмотрите значение переменной msg1 по имени Посмотрите 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. Измените первый символ переменной msg1 Замените любой символ во второй переменной msg2. (рис. 2.12)

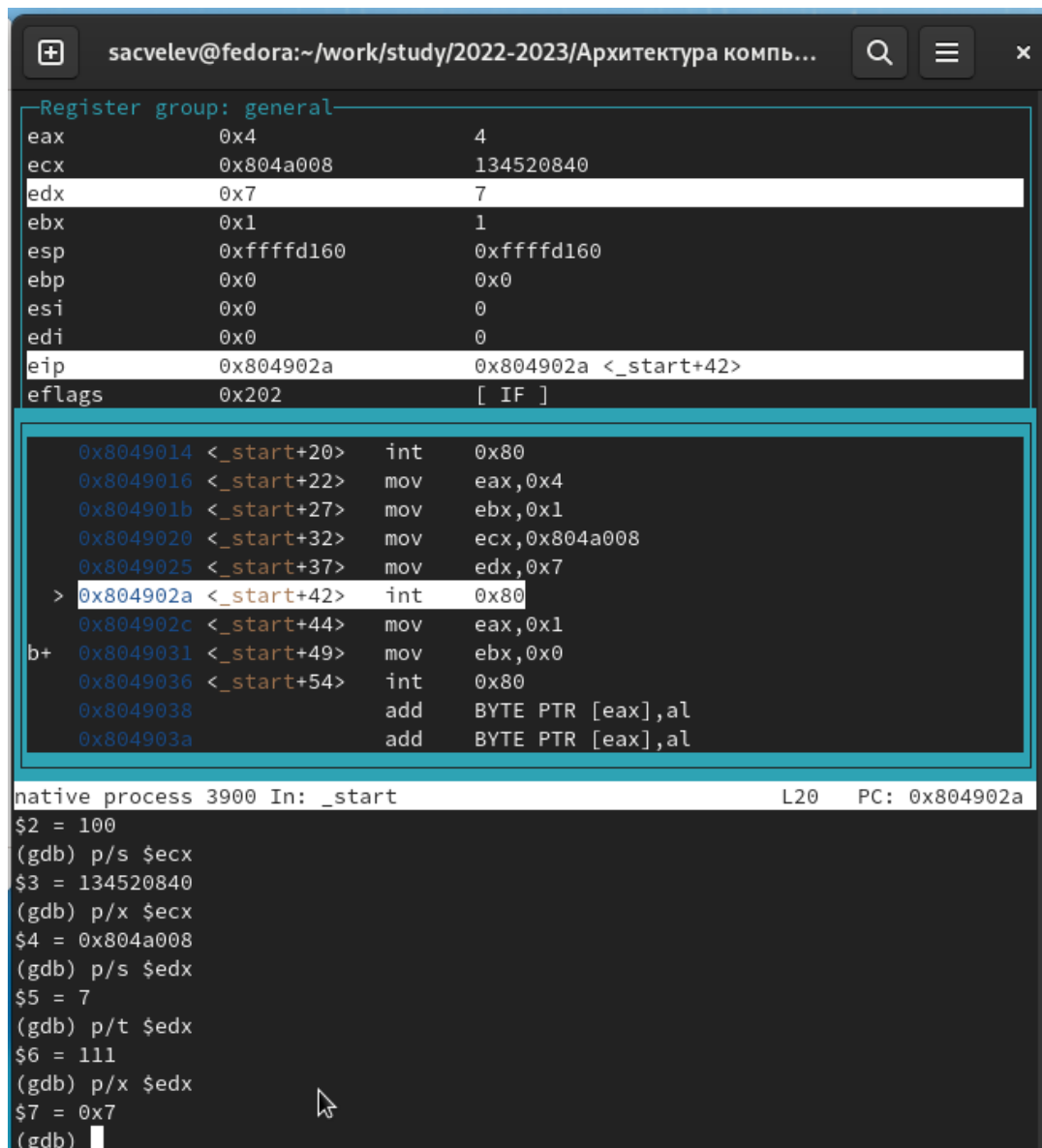
```
sacvelev@fedora:~/work/study/2022-2023/Архитектура компь...
Register group: general
eax      0x4      4
ecx      0x804a008 134520840
edx      0x7      7
ebx      0x1      1
esp      0xffffd160 0xffffd160
ebp      0x0      0x0
esi      0x0      0
edi      0x0      0
eip      0x804902a 0x804902a <_start+42>
eflags   0x202    [ IF ]

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
0x8049036 <_start+54> int 0x80
0x8049038      add BYTE PTR [eax],al
0x804903a      add BYTE PTR [eax],al

native process 3900 In: _start L20 PC: 0x804902a
(gdb) si
(gdb) x/1sb &msg1
0x804a000 <msg1>: "Hello, "
(gdb) x/1sb 0x804a008
0x804a008 <msg2>: "world!\n\034"
(gdb) set {char}&msg1='h'
(gdb) x/1sb &msg1
0x804a000 <msg1>: "hello, "
(gdb) set {char}0x804a008='L'
(gdb) x/1sb 0x804a008
0x804a008 <msg2>: "Lor!d!\n\034"
(gdb) 
```

Рис. 2.12: изменение значения переменной

Выведете в различных форматах (в шестнадцатеричном формате, в двоичном формате и в символьном виде) значение регистра edx. С помощью команды set измените значение регистра ebx:(рис. 2.13)



```
sacvelev@fedora:~/work/study/2022-2023/Архитектура компь...
Register group: general
eax      0x4      4
ecx      0x804a008 134520840
edx      0x7      7
ebx      0x1      1
esp      0xffffd160 0xffffd160
ebp      0x0      0x0
esi      0x0      0
edi      0x0      0
eip      0x804902a 0x804902a <_start+42>
eflags   0x202    [ IF ]

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
0x8049036 <_start+54> int 0x80
0x8049038 add BYTE PTR [eax],al
0x804903a add BYTE PTR [eax],al

native process 3900 In: _start L20 PC: 0x804902a
$2 = 100
(gdb) p/s $ecx
$3 = 134520840
(gdb) p/x $ecx
$4 = 0x804a008
(gdb) p/s $edx
$5 = 7
(gdb) p/t $edx
$6 = 111
(gdb) p/x $edx
$7 = 0x7
(gdb)
```

Рис. 2.13: вывод значения регистра

С помощью команды set измените значение регистра ebx:(рис. 2.14)

The screenshot shows a GDB terminal window with the title bar "sacvelev@fedora:~/work/study/2022-2023/Архитектура компь...". The window is divided into three main sections. The top section, titled "Register group: general", lists the values of general-purpose registers: eax (0x4), ecx (0x804a008), edx (0x7), ebx (0x2), esp (0xffffd160), ebp (0x0), esi (0x0), edi (0x0), eip (0x804902a), and eflags (0x202). The middle section displays assembly code with addresses and instructions, such as "0x8049014 <_start+20> int 0x80" and "0x804902a <_start+42> int 0x80". The bottom section shows the GDB command prompt with various commands like "p/t \$edx", "p/x \$edx", "set \$ebx='2'", and "p/s \$ebx".

```
Register group: general
eax      0x4      4
ecx      0x804a008 134520840
edx      0x7      7
ebx      0x2      2
esp      0xffffd160 0xffffd160
ebp      0x0      0x0
esi      0x0      0
edi      0x0      0
eip      0x804902a 0x804902a <_start+42>
eflags   0x202    [ IF ]

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
0x8049036 <_start+54> int 0x80
0x8049038 add BYTE PTR [eax],al
0x804903a add BYTE PTR [eax],al

native process 3900 In: _start L20 PC: 0x804902a
$5 = 7
(gdb) p/t $edx
$6 = 111
(gdb) p/x $edx
$7 = 0x7
(gdb) set $ebx='2'
(gdb) p/s $ebx
$8 = 50
(gdb) set $ebx=2
(gdb) p/s $ebx
$9 = 2
(gdb)
```

Рис. 2.14: вывод значения регистра

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

Для начала установим точку останова перед первой инструкцией в программе

и запустим ее.

Адрес вершины стека храниться 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’`.

Посмотрите остальные позиции стека – по адресу `[esp+4]` располагается адрес в памяти где находится имя программы, по адресу `[esp+8]` храниться адрес первого аргумента, по адресу `[esp+12]` – второго и т.д. (рис. 2.15)

```
sacvelev@fedora:~/work/study/2022-2023/Архитектура компь...
Reading symbols from lab10-3...
(gdb) b _start
Breakpoint 1 at 0x80490e8: file lab10-3.asm, line 5.
(gdb) r
Starting program: /home/sacvelev/work/study/2022-2023/Архитектура компьютера/arch
h-pc/labs/lab10/lab10-3 argument 1 argument 2 argument\ 3

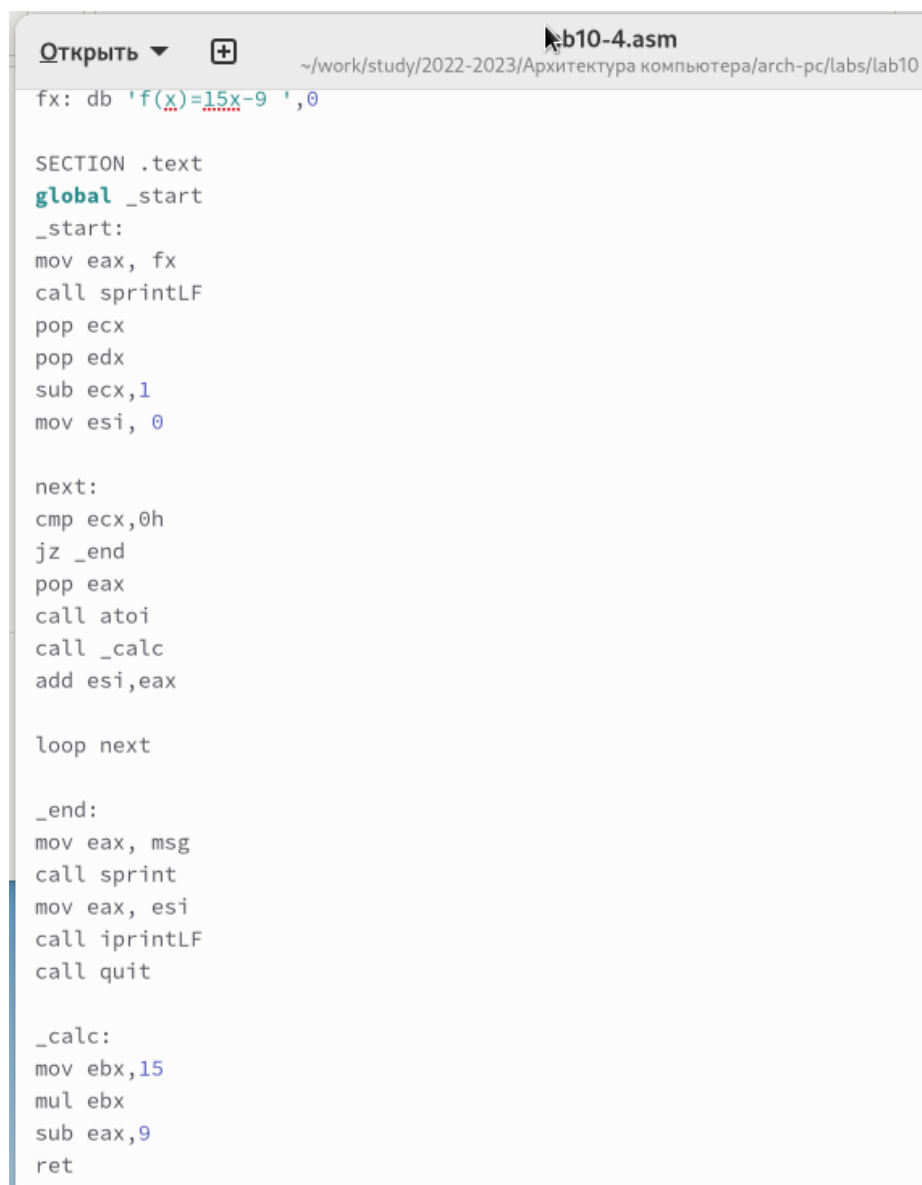
This GDB supports auto-downloading debuginfo from the following URLs:
https://debuginfod.fedoraproject.org/
Enable debuginfod for this session? (y or [n])
Debuginfod has been disabled.
To make this setting permanent, add 'set debuginfod enabled off' to .gdbinit.

Breakpoint 1, _start () at lab10-3.asm:5
5      pop ecx ; Извлекаем из стека в `ecx` количество
(gdb) b _start
Note: breakpoint 1 also set at pc 0x80490e8.
Breakpoint 2 at 0x80490e8: file lab10-3.asm, line 5.
(gdb) x/x $esp
0xffffd130:      0x00000006
(gdb) x/s *(void**)( $esp + 4)
0xffffd2ea:      "/home/sacvelev/work/study/2022-2023/Архитектура компьютера/arch
-pc/labs/lab10/lab10-3"
(gdb) x/s *(void**)( $esp + 4)
0xffffd2ea:      "/home/sacvelev/work/study/2022-2023/Архитектура компьютера/arch
-pc/labs/lab10/lab10-3"
(gdb) x/s *(void**)( $esp + 8)
0xffffd355:      "argument"
(gdb) x/s *(void**)( $esp + 12)
0xffffd35e:      "1"
(gdb) x/s *(void**)( $esp + 16)
0xffffd360:      "argument"
(gdb) x/s *(void**)( $esp + 20)
0xffffd369:      "2"
(gdb) x/s *(void**)( $esp + 24)
0xffffd36b:      "argument 3"
(gdb)
```

Рис. 2.15: вывод значения регистра

Объясните, почему шаг изменения адреса равен 4 ([esp+4], [esp+8], [esp+12] - шаг равен размеру переменной - 4 байтам.

- Преобразуйте программу из лабораторной работы №9 (Задание №1 для самостоятельной работы), реализовав вычисление значения функции $f(x)$ как подпрограмму. (рис. 2.16 2.17)



```
Открыть ▾ + b10-4.asm
~/work/study/2022-2023/Архитектура компьютера/arch-pc/labs/lab10

fx: db 'f(x)=15x-9 ',0

SECTION .text
global _start
_start:
mov eax, fx
call sprintf
pop ecx
pop edx
sub ecx,1
mov esi, 0

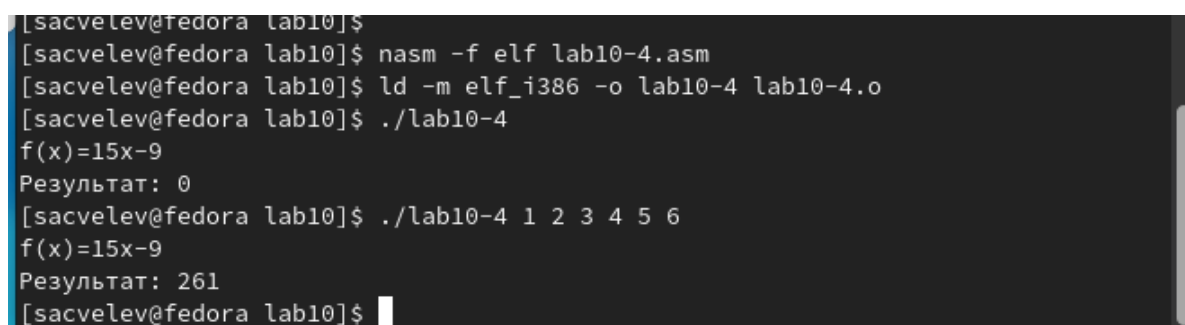
next:
cmp ecx,0h
jz _end
pop eax
call atoi
call _calc
add esi,eax

loop next

_end:
mov eax, msg
call sprintf
mov eax, esi
call iprintLF
call quit

_calc:
mov ebx,15
mul ebx
sub eax,9
ret
```

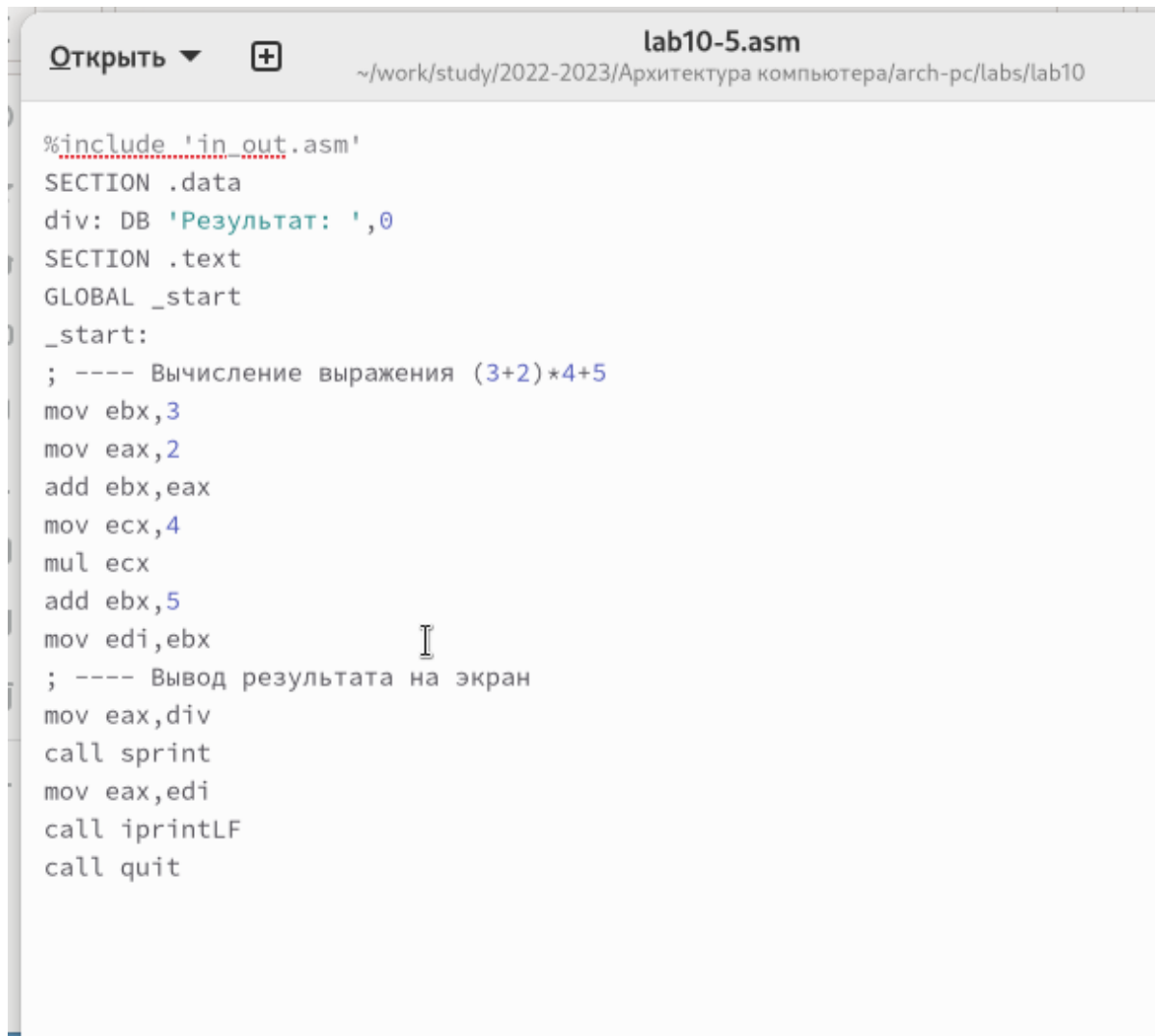
Рис. 2.16: Файл lab10-4.asm



```
[sacvelev@fedora lab10]$
[sacvelev@fedora lab10]$ nasm -f elf lab10-4.asm
[sacvelev@fedora lab10]$ ld -m elf_i386 -o lab10-4 lab10-4.o
[sacvelev@fedora lab10]$ ./lab10-4
f(x)=15x-9
Результат: 0
[sacvelev@fedora lab10]$ ./lab10-4 1 2 3 4 5 6
f(x)=15x-9
Результат: 261
[sacvelev@fedora lab10]$
```

Рис. 2.17: Работа программы lab10-4.asm

7. В листинге приведена программа вычисления выражения $(3+2)*4+5$. При запуске данная программа дает неверный результат. Проверьте это. С помощью отладчика GDB, анализируя изменения значений регистров, определите ошибку и исправьте ее. (рис. 2.18 2.19 2.20 2.21)



```
lab10-5.asm
~/work/study/2022-2023/Архитектура компьютера/arch-pc/labs/lab10

%include 'in_out.asm'
SECTION .data
div: DB 'Результат: ',0
SECTION .text
GLOBAL _start
_start:
; ---- Вычисление выражения (3+2)*4+5
mov ebx,3
mov eax,2
add ebx,eax
mov ecx,4
mul ecx
add ebx,5
mov edi,ebx
; ---- Вывод результата на экран
mov eax,div
call sprint
mov eax,edi
call iprintLF
call quit
```

Рис. 2.18: код с ошибкой


```
sacvelev@fedora:~/work/study/2022-2023/Архитектура компь...
eax      0x804a002      134520834
ecx      0x4           4
edx      0x0           0
ebx      0x804a000      134520832
esp      0xffffd144    0xffffd144
ebp      0x0           0x0
esi      0x0           0
edi      0xa           10
eip      0x8049006      0x8049006 <nextchar+3>
eflags   0x282         [ SF IF ]

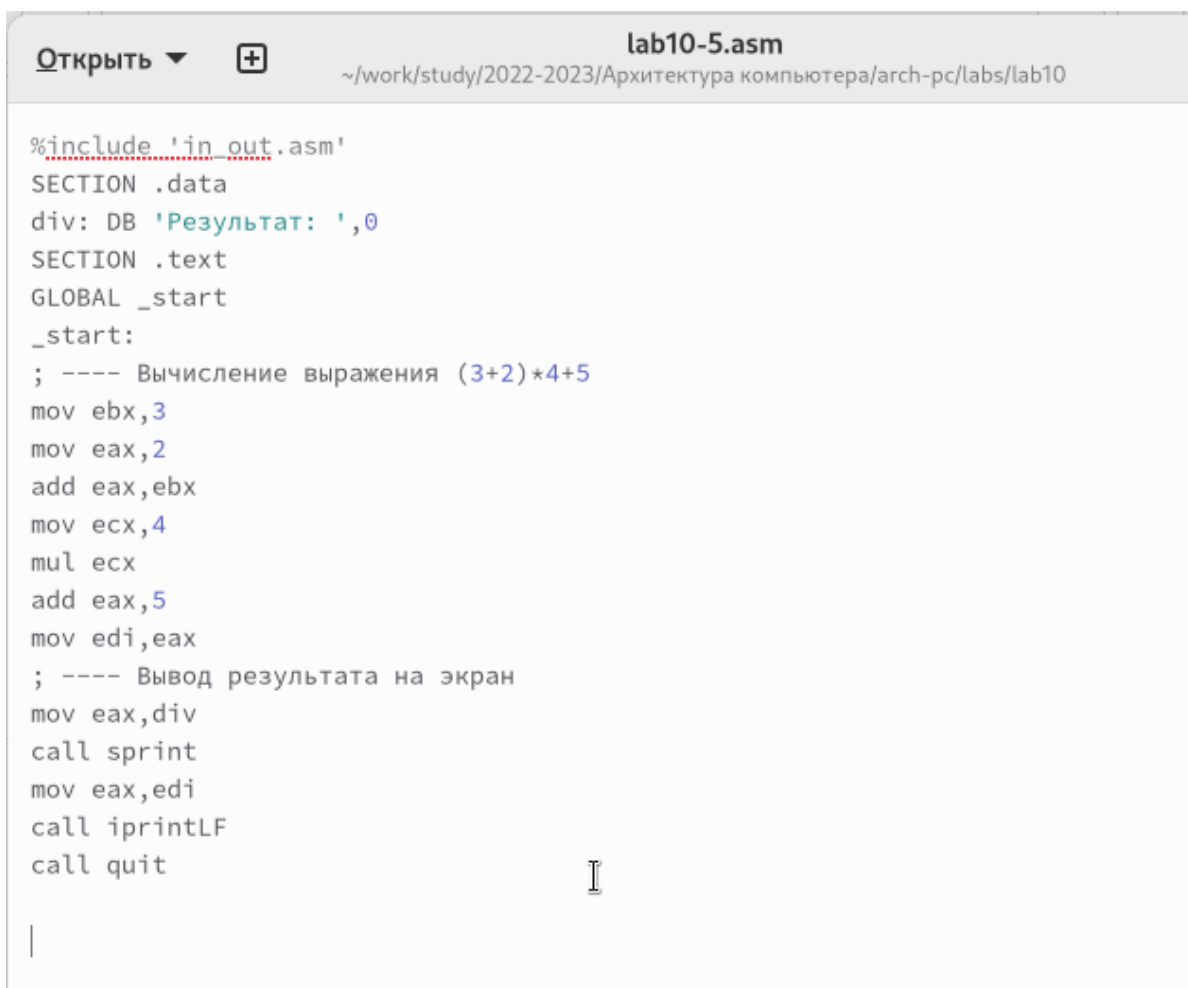
0x8049000 <slen>      push    ebx
0x8049006 <nextchar+3> je      0x804900b <finished>
0x8049009 <nextchar+6> jmp     0x8049003 <nextchar>
0x804900b <finished>  sub     eax,ebx
0x804900d <finished+2> pop     ebx
0x804900e <finished+3> ret
0x804900f <sprint>    push    edx
0x8049010 <sprint+1>  push    ecx

0x8049011 <sprint+2>  push    ebx
0x8049012 <sprint+3>  push    eax
0x8049013 <sprint+4>  call    0x8049000 <slen>

native process 4279 In: nextchar      L10  PC: 0x8049006
(gdb) sNo process In:                L??  PC: ??
(gdb) si
(gdb) si
(gdb) si
(gdb) si
(gdb) si
(gdb) si
(gdb) si
(gdb) si
(gdb) cont
Continuing.
Результат: 10
[Inferior 1 (process 4279) exited normally]
(gdb)
```

Рис. 2.19: отладка

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



```
lab10-5.asm
~/work/study/2022-2023/Архитектура компьютера/arch-pc/labs/lab10

%include 'in_out.asm'
SECTION .data
div: DB 'Результат: ',0
SECTION .text
GLOBAL _start
_start:
; ---- Вычисление выражения (3+2)*4+5
mov ebx,3
mov eax,2
add eax,ebx
mov ecx,4
mul ecx
add eax,5
mov edi,eax
; ---- Вывод результата на экран
mov eax,div
call sprint
mov eax,edi
call iprintLF
call quit
```

Рис. 2.20: код исправлен

```
sacvelev@fedora:~/work/study/2022-2023/Архитектура компь...
eax      0x19      25
ecx      0x4       4
edx      0x0       0
ebx      0x3       3
esp      0xffffd160 0xffffd160
ebp      0x0       0x0
esi      0x0       0
edi      0x0       0
eip      0x80490fe 0x80490fe <_start+22>
eflags   0x202     [ IF ]

B+ 0x80490e8 <_start>    mov     ebx,0x3
0x80490fe <_start+22>    mov     edi,eax
0x8049100 <_start+24>    add     eax,eb804a000
0x8049105 <_start+29>    call   0x804900f <sprint>
0x804910a <_start+34>    mul     eax,edi
0x804910c <_start+36>    call   0x8049086 <iprintLF>
> 0x8049111 <_start+41>    call   0x80490db <quit>
                                04a000
                                rint>
                                86 <iprintLF>

native process 4369 In: _start L14 PC: 0x80490fe
To makeNo process In: , add 'set debuginfod enabled' L?? PC: ??
Breakpoint 1, _start () at lab10-5.asm:8
(gdb) si
(gdb) si
(gdb) si
(gdb) si
(gdb) si
(gdb) si
(gdb) cont
Continuing.
Результат: 25
[Inferior 1 (process 4369) exited normally]
(gdb)
```

Рис. 2.21: проверка работы

3 Выводы

Освоили работу с подпрограммами и отладчиком.