

Отчёт по лабораторной работе 9

Дисциплина: Архитектура компьютеров

Баранов Георгий Павлович

Содержание

1	Цель работы	5
2	Теоретическое введение	6
3	Выполнение лабораторной работы	7
3.1	Реализация подпрограмм в NASM	7
3.2	Отладка программ с помощью GDB	11
3.3	Задание для самостоятельной работы	22
4	Выводы	29

Список иллюстраций

3.1	Программа в файле lab9-1.asm	8
3.2	Запуск программы lab9-1.asm	9
3.3	Программа в файле lab9-1.asm	10
3.4	Запуск программы lab9-1.asm	10
3.5	Программа в файле lab9-2.asm	11
3.6	Запуск программы lab9-2.asm в отладчике	12
3.7	Дизассимилированный код	13
3.8	Дизассимилированный код в режиме интел	14
3.9	Точка остановки	15
3.10	Изменение регистров	16
3.11	Изменение регистров	17
3.12	Изменение значения переменной	18
3.13	Вывод значения регистра	19
3.14	Вывод значения регистра	20
3.15	Программа в файле lab9-3.asm	21
3.16	Вывод значения регистра	22
3.17	Программа в файле task-1.asm	23
3.18	Запуск программы task-1.asm	24
3.19	Код с ошибкой в файле task-2.asm	25
3.20	Отладка task-2.asm	26
3.21	Код исправлен в файле task-2.asm	27
3.22	Проверка работы task-2.asm	28

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 Теоретическое введение

Отладка — это процесс поиска и исправления ошибок в программе. В общем случае его можно разделить на четыре этапа:

- обнаружение ошибки;
- поиск её местонахождения;
- определение причины ошибки;
- исправление ошибки.

GDB (GNU Debugger — отладчик проекта GNU) работает на многих UNIX-подобных системах и умеет производить отладку многих языков программирования. GDB предлагает обширные средства для слежения и контроля за выполнением компьютерных программ. Отладчик не содержит собственного графического пользовательского интерфейса и использует стандартный текстовый интерфейс консоли. Однако для GDB существует несколько сторонних графических надстроек, а кроме того, некоторые интегрированные среды разработки используют его в качестве базовой подсистемы отладки. Отладчик GDB (как и любой другой отладчик) позволяет увидеть, что происходит «внутри» программы в момент её выполнения или что делает программа в момент сбоя.

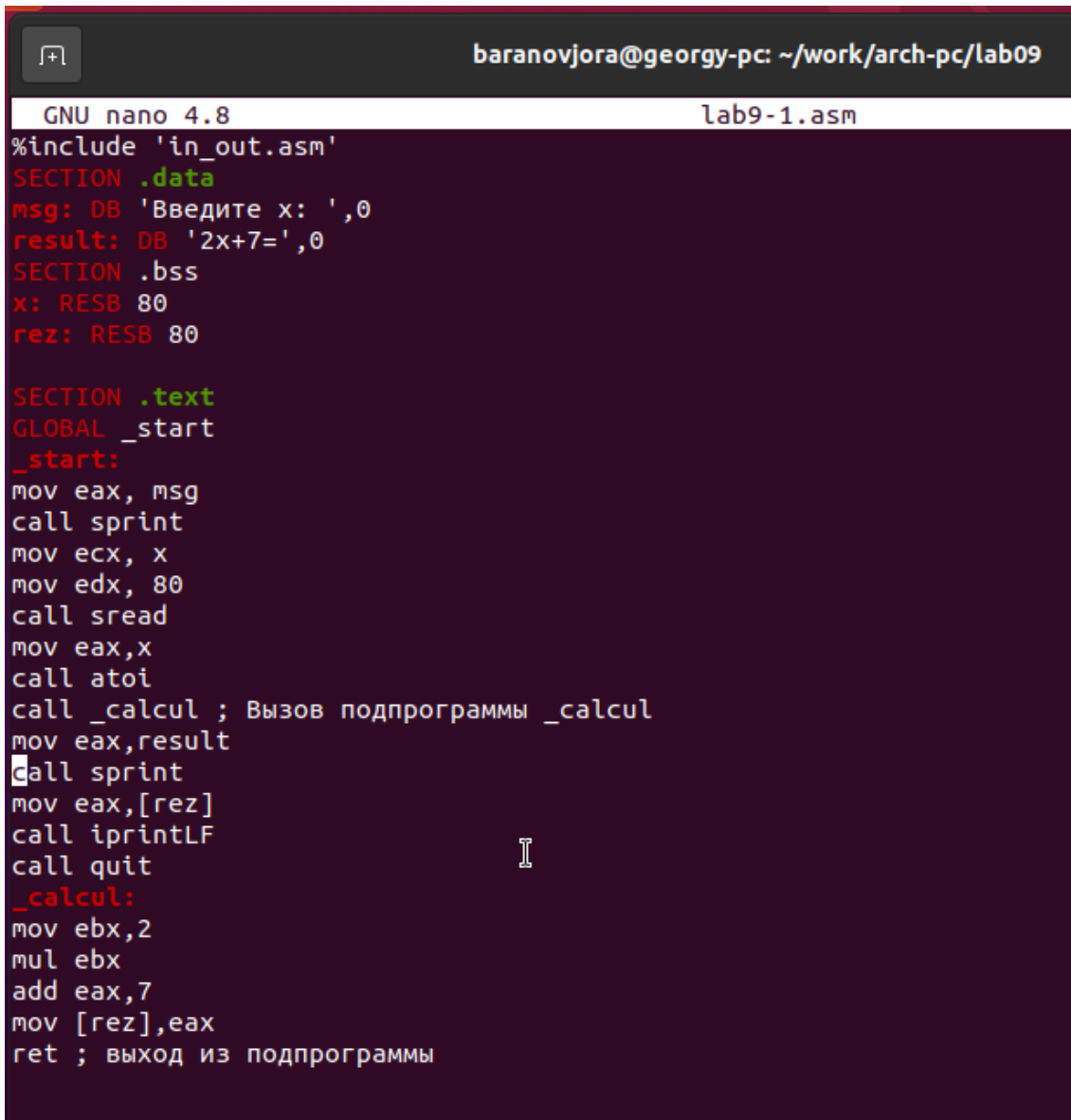
Подпрограмма — это, как правило, функционально законченный участок кода, который можно многократно вызывать из разных мест программы. В отличие от простых переходов из подпрограмм существует возврат на команду, следующую за вызовом

3 Выполнение лабораторной работы

3.1 Реализация подпрограмм в NASM

Я создал каталог для выполнения лабораторной работы №9 и перешел в него.

В качестве примера рассмотрим программу, которая вычисляет арифметическое выражение $f(x) = 2x + 7$ с использованием подпрограммы `calcul`. В этом примере значение x вводится с клавиатуры, а само выражение вычисляется в подпрограмме.



```
baranovjora@georgy-pc: ~/work/arch-pc/lab09
GNU nano 4.8 lab9-1.asm
#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. 3.1: Программа в файле lab9-1.asm

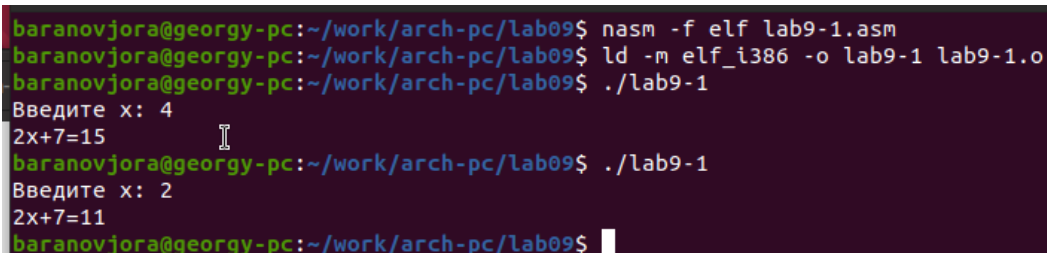
Первые строки программы отвечают за вывод сообщения на экран (с помощью вызова `sprint`), чтение данных, введенных с клавиатуры (с помощью вызова `sread`) и преобразование введенных данных из символьного вида в численный (с помощью вызова `atoi`).

После инструкции `call _calcul`, которая передает управление подпрограмме `_calcul`, будут выполнены инструкции, содержащиеся в подпрограмме.

Инструкция `ret` является последней в подпрограмме и ее выполнение приводит

к возврату в основную программу к инструкции, следующей за инструкцией call, которая вызвала данную подпрограмму.

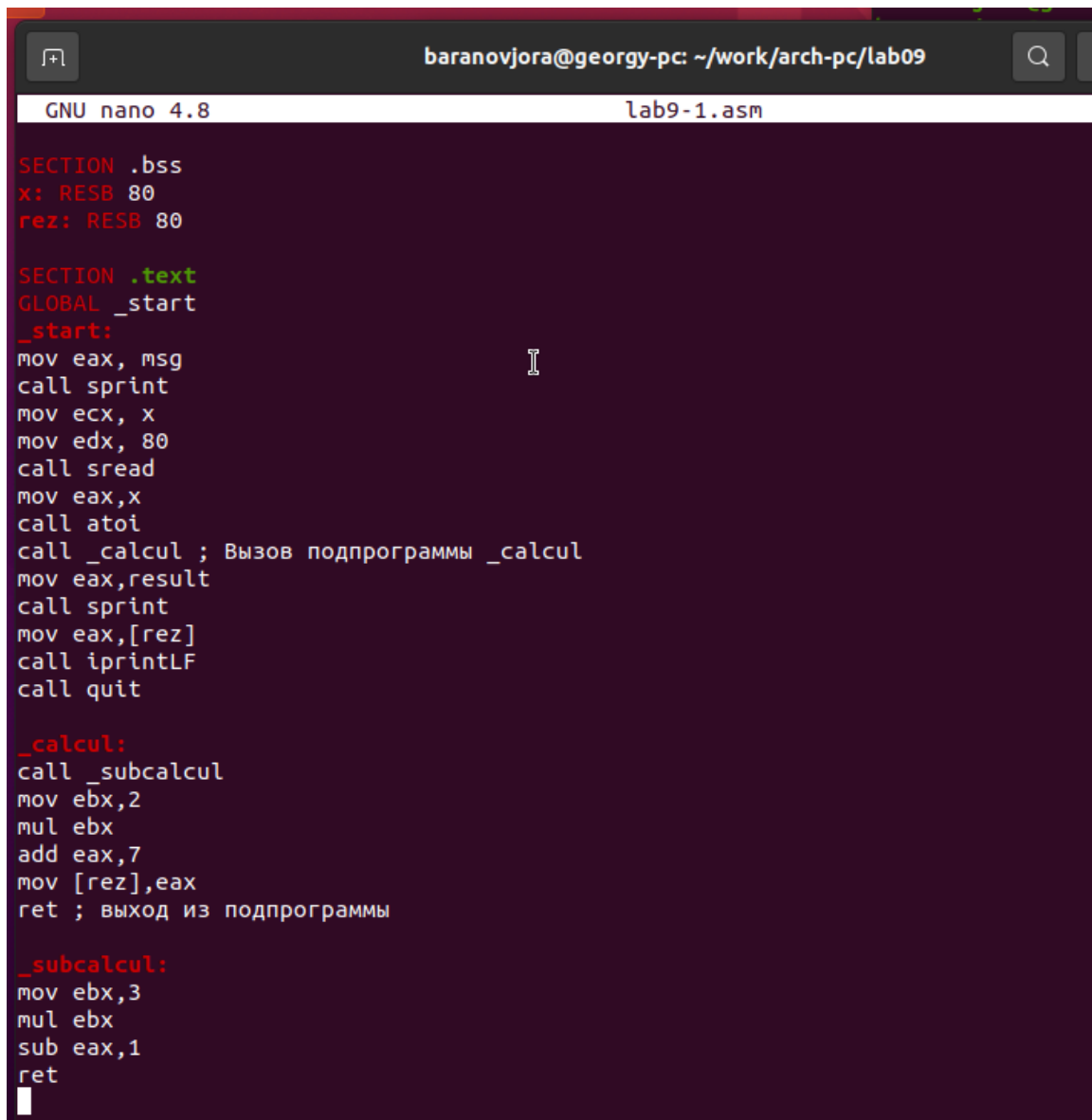
Последние строки программы реализуют вывод сообщения (с помощью вызова sprint), вывод результата вычисления (с помощью вызова iprintLF) и завершение программы (с помощью вызова quit).



```
baranovjora@georgy-pc:~/work/arch-pc/lab09$ nasm -f elf lab9-1.asm
baranovjora@georgy-pc:~/work/arch-pc/lab09$ ld -m elf_i386 -o lab9-1 lab9-1.o
baranovjora@georgy-pc:~/work/arch-pc/lab09$ ./lab9-1
Введите x: 4
2x+7=15
baranovjora@georgy-pc:~/work/arch-pc/lab09$ ./lab9-1
Введите x: 2
2x+7=11
baranovjora@georgy-pc:~/work/arch-pc/lab09$
```

Рис. 3.2: Запуск программы lab9-1.asm

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



```
baranovjora@georgy-pc: ~/work/arch-pc/lab09
GNU nano 4.8 lab9-1.asm

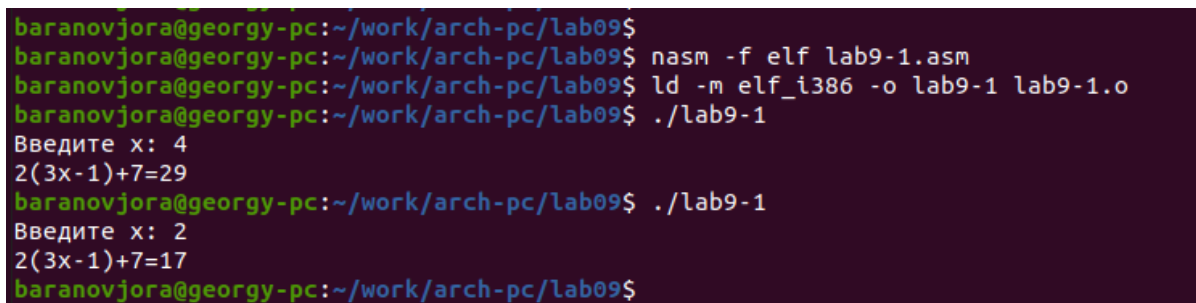
SECTION .bss
x: RESB 80
rez: RESB 80

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. 3.3: Программа в файле lab9-1.asm

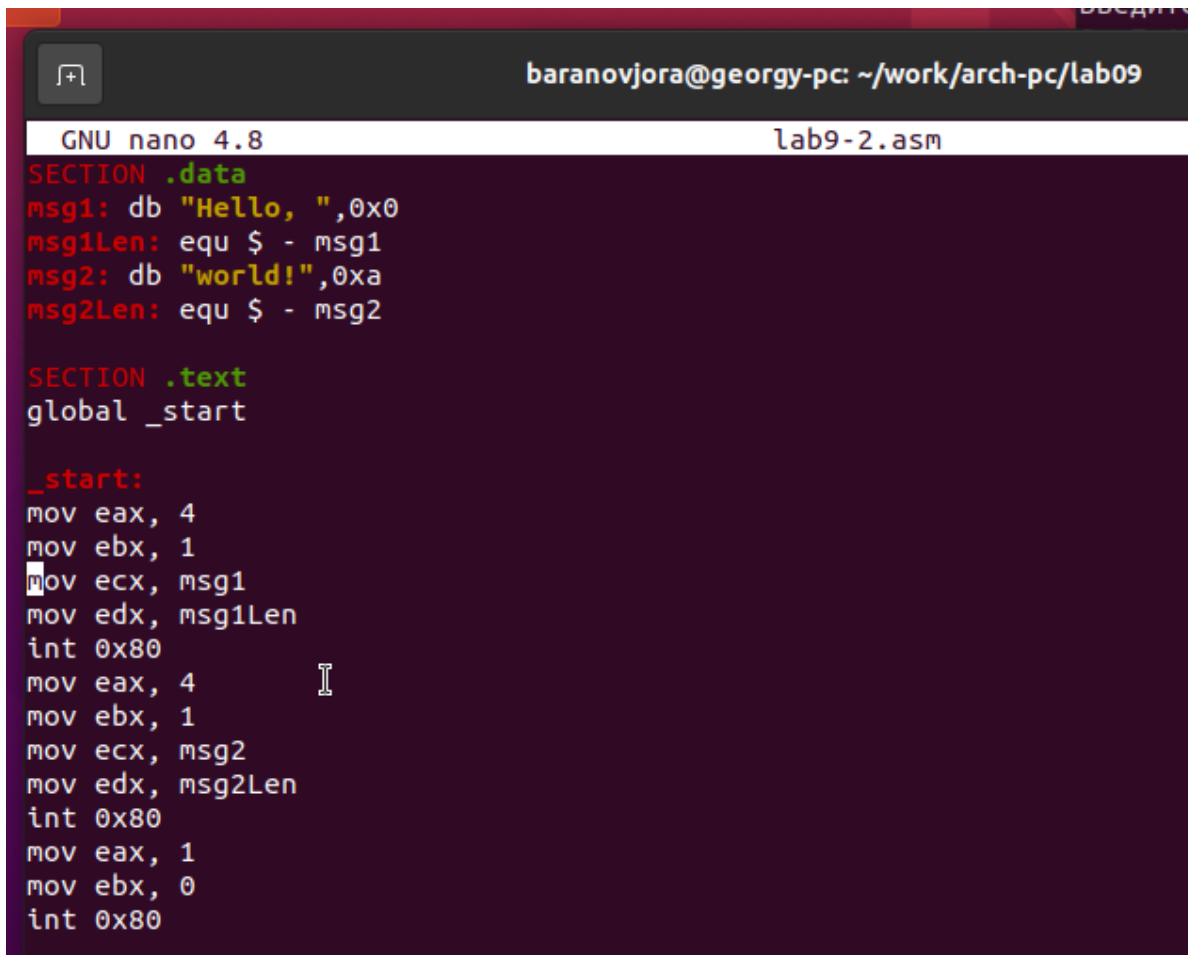


```
baranovjora@georgy-pc:~/work/arch-pc/lab09$
baranovjora@georgy-pc:~/work/arch-pc/lab09$ nasm -f elf lab9-1.asm
baranovjora@georgy-pc:~/work/arch-pc/lab09$ ld -m elf_i386 -o lab9-1 lab9-1.o
baranovjora@georgy-pc:~/work/arch-pc/lab09$ ./lab9-1
Введите x: 4
2(3x-1)+7=29
baranovjora@georgy-pc:~/work/arch-pc/lab09$ ./lab9-1
Введите x: 2
2(3x-1)+7=17
baranovjora@georgy-pc:~/work/arch-pc/lab09$
```

Рис. 3.4: Запуск программы lab9-1.asm

3.2 Отладка программ с помощью GDB

Создал файл lab9-2.asm с текстом программы из Листинга 9.2. (Программа печати сообщения Hello world!).



```
baranovjora@georgy-pc: ~/work/arch-pc/lab09
GNU nano 4.8 lab9-2.asm
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. 3.5: Программа в файле lab9-2.asm

Получил исполняемый файл. Для работы с GDB в исполняемый файл необходимо добавить отладочную информацию, для этого трансляцию программ необходимо проводить с ключом '-g'.

Загрузил исполняемый файл в отладчик gdb. Проверил работу программы, запустив ее в оболочке GDB с помощью команды run (сокращённо r).

```

baranovjora@georgy-pc:~/work/arch-pc/lab09$
baranovjora@georgy-pc:~/work/arch-pc/lab09$ nasm -f elf -g -l lab9-2.lst lab9-2.asm
baranovjora@georgy-pc:~/work/arch-pc/lab09$ ld -m elf_i386 -o lab9-2 lab9-2.o
baranovjora@georgy-pc:~/work/arch-pc/lab09$ gdb lab9-2
GNU gdb (Ubuntu 9.2-0ubuntu1~20.04.2) 9.2
Copyright (C) 2020 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-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://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 lab9-2...
(gdb) run
Starting program: /home/baranovjora/work/arch-pc/lab09/lab9-2
Hello, world!
[Inferior 1 (process 2202) exited normally]
(gdb) █

```

Рис. 3.6: Запуск программы lab9-2.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.

```
baranovjora@georgy-pc: ~/work/arch-pc/lab09
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-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://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 lab9-2...
(gdb) run
Starting program: /home/baranovjora/work/arch-pc/lab09/lab9-2
Hello, world!
[Inferior 1 (process 2202) exited normally]
(gdb) break _start
Breakpoint 1 at 0x08049000
(gdb) r
Starting program: /home/baranovjora/work/arch-pc/lab09/lab9-2

Breakpoint 1, 0x08049000 in _start ()
(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. 3.7: Дизассимилированный код

```
baranovjora@georgy-pc: ~/work/arch-pc/lab09
[Inferior 1 (process 2202) exited normally]
(gdb) break _start
Breakpoint 1 at 0x8049000
(gdb) r
Starting program: /home/baranovjora/work/arch-pc/lab09/lab9-2

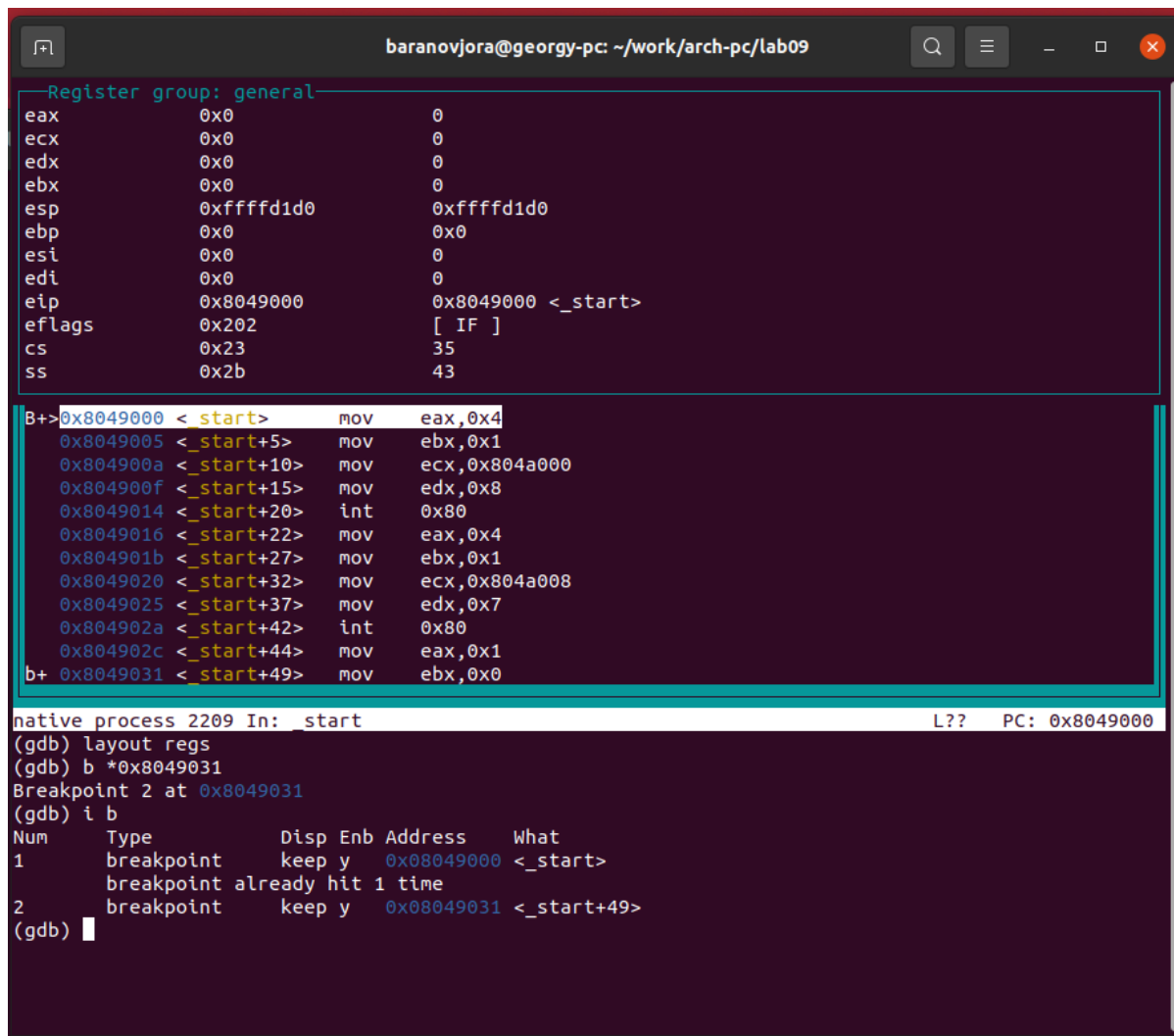
Breakpoint 1, 0x08049000 in _start ()
(gdb) disassemble _start
Dump of assembler code for function _start:
=> 0x08049000 <+0>:    mov     $0x4,%eax
      0x08049005 <+5>:    mov     $0x1,%ebx
      0x0804900a <+10>:   mov     $0x804a000,%ecx
      0x0804900f <+15>:   mov     $0x8,%edx
      0x08049014 <+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) 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: Дизассимилированный код в режиме интел

Установить точку останова можно командой `break` (кратко `b`). Типичный аргумент этой команды — место установки. Его можно задать или как номер строки программы (имеет смысл, если есть исходный файл, а программа компилировалась с информацией об отладке), или как имя метки, или как адрес. Чтобы не было путаницы с номерами, перед адресом ставится «звёздочка»

На предыдущих шагах была установлена точка останова по имени метки (`_start`). Проверил это с помощью команды `info breakpoints` (кратко `i b`). Установил еще одну точку останова по адресу инструкции. Адрес инструкции можно увидеть в средней части экрана в левом столбце соответствующей инструкции.

Определил адрес предпоследней инструкции (mov ebx,0x0) и установил точку.



```
baranovjora@georgy-pc: ~/work/arch-pc/lab09

Register group: general
eax      0x0      0
ecx      0x0      0
edx      0x0      0
ebx      0x0      0
esp      0xffffd1d0 0xffffd1d0
ebp      0x0      0x0
esi      0x0      0
edi      0x0      0
eip      0x8049000 0x8049000 <_start>
eflags   0x202    [ IF ]
cs       0x23     35
ss       0x2b     43

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 2209 In: _start L?? PC: 0x8049000
(gdb) layout regs
(gdb) b *0x8049031
Breakpoint 2 at 0x8049031
(gdb) i b
Num    Type           Disp Enb Address      What
1      breakpoint     keep y  0x08049000 <_start>
       breakpoint already hit 1 time
2      breakpoint     keep y  0x08049031 <_start+49>
(gdb)
```

Рис. 3.9: Точка остановки

Отладчик может показывать содержимое ячеек памяти и регистров, а при необходимости позволяет вручную изменять значения регистров и переменных. Выполнил 5 инструкций с помощью команды stepi (или si) и проследил за изменением значений регистров.

```
baranovjora@georgy-pc: ~/work/arch-pc/lab09

Register group: general
eax      0x4      4
ecx      0x0      0
edx      0x0      0
ebx      0x0      0
esp      0xffffd1d0 0xffffd1d0
ebp      0x0      0x0
esi      0x0      0
edi      0x0      0
eip      0x8049005 0x8049005 < start+5>
eflags   0x202    [ IF ]
cs       0x23     35
ss       0x2b     43

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 2209 In: _start L?? PC: 0x8049005
edi      0x0      0
eip      0x8049000 0x8049000 < _start>
eflags   0x202    [ IF ]
cs       0x23     35
ss       0x2b     43
--Type <RET> for more, q to quit, c to continue without paging--
ds       0x2b     43
es       0x2b     43
fs       0x0      0
gs       0x0      0
(gdb) si
0x08049005 in _start ()
(gdb) █
```

Рис. 3.10: Изменение регистров


```
baranovjora@georgy-pc: ~/work/arch-pc/lab09

Register group: general
eax      0x8      8
ecx      0x804a000 134520832
edx      0x8      8
ebx      0x1      1
esp      0xffffd1d0 0xffffd1d0
ebp      0x0      0x0
esi      0x0      0
edi      0x0      0
eip      0x8049016 0x8049016 <_start+22>
eflags   0x202    [ IF ]
cs       0x23     35
ss       0x2b     43

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 2209 In: _start L?? PC: 0x8049016
fs      0x0      0
gs      0x0      0
(gdb) si
0x08049005 in _start ()
(gdb) si
0x0804900a in _start ()
(gdb) si
0x0804900f in _start ()
(gdb) si
0x08049014 in _start ()
(gdb) si
0x08049016 in _start ()
(gdb) █
```

Рис. 3.11: Изменение регистров

Посмотрел значение переменной `msg1` по имени. Посмотрел 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. Изменил первый символ переменной `msg1`.

```
baranovjora@georgy-pc: ~/work/arch-pc/lab09

Register group: general
eax      0x8      8
ecx      0x804a000 134520832
edx      0x8      8
ebx      0x1      1
esp      0xffffd1d0 0xffffd1d0
ebp      0x0      0x0
esi      0x0      0
edi      0x0      0
eip      0x8049016 0x8049016 < start+22>
eflags   0x202    [ IF ]
cs       0x23     35
ss       0x2b     43

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 2209 In: _start L?? PC: 0x8049016
(gdb) si
0x8049016 in _start ()
(gdb) x/1sb &msg1
0x804a000 <msg1>:      "Hello, "
(gdb) x/1sb 0x804a008
0x804a008 <msg2>:      "world!\n"
(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"
(gdb) 
```

Рис. 3.12: Изменение значения переменной

Вывел в различных форматах (в шестнадцатеричном формате, в двоичном формате и в символьном виде) значение регистра edx.

```
baranovjora@georgy-pc: ~/work/arch-pc/lab09

Register group: general
eax      0x8      8
ecx      0x804a000 134520832
edx      0x8      8
ebx      0x1      1
esp      0xffffd1d0 0xffffd1d0
ebp      0x0      0x0
esi      0x0      0
edi      0x0      0
eip      0x8049016 0x8049016 < start+22>
eflags   0x202    [ IF ]
cs       0x23     35
ss       0x2b     43

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 2209 In: _start L?? PC: 0x8049016
(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 изменил значение регистра ebx

```
baranovjora@georgy-pc: ~/work/arch-pc/lab09

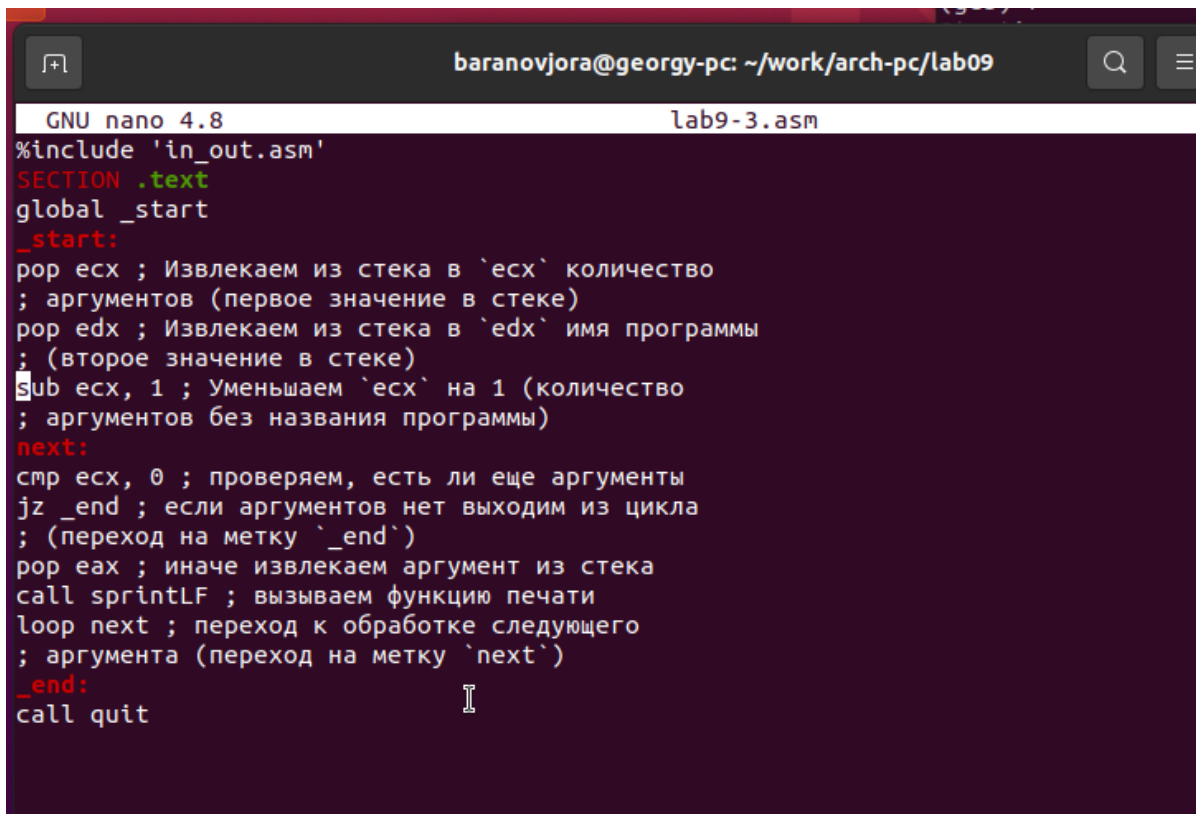
Register group: general
eax      0x8      8
ecx      0x804a000 134520832
edx      0x8      8
ebx      0x2      2
esp      0xffffd1d0 0xffffd1d0
ebp      0x0      0x0
esi      0x0      0
edi      0x0      0
eip      0x8049016 0x8049016 <_start+22>
eflags   0x202    [ IF ]
cs       0x23     35
ss       0x2b     43

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 2209 In: _start L?? PC: 0x8049016
(gdb) p/s $edx
$5 = 8
(gdb) p/t $edx
$6 = 1000
(gdb) p/x $edx
$7 = 0x8
(gdb) set $ebx='2'
(gdb) p/s $ebx
$8 = 50
(gdb) set $ebx=2
(gdb) p/s $ebx
$9 = 2
(gdb) █
```

Рис. 3.14: Вывод значения регистра

Скопировал файл lab8-2.asm, созданный при выполнении лабораторной работы №8, с программой выводящей на экран аргументы командной строки. Создал исполняемый файл. Для загрузки в gdb программы с аргументами необходимо использовать ключ `-args`. Загрузил исполняемый файл в отладчик, указав аргументы.



```
GNU nano 4.8 lab9-3.asm
#include 'in_out.asm'
SECTION .text
global _start
_start:
pop ecx ; Извлекаем из стека в `ecx` количество
; аргументов (первое значение в стеке)
pop edx ; Извлекаем из стека в `edx` имя программы
; (второе значение в стеке)
sub ecx, 1 ; Уменьшаем `ecx` на 1 (количество
; аргументов без названия программы)
next:
cmp ecx, 0 ; проверяем, есть ли еще аргументы
jz _end ; если аргументов нет выходим из цикла
; (переход на метку `_end`)
pop eax ; иначе извлекаем аргумент из стека
call sprintLF ; вызываем функцию печати
loop next ; переход к обработке следующего
; аргумента (переход на метку `next`)
_end:
call quit
```

Рис. 3.15: Программа в файле lab9-3.asm

Для начала установил точку останова перед первой инструкцией в программе и запустил 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 lab9-3 и непосредственно аргументы: аргумент1, аргумент, 2 и ‘аргумент 3’.

Посмотрел 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.

```
baranovjora@georgy-pc: ~/work/arch-pc/lab09
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://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 lab9-3...
(gdb) b _start
Breakpoint 1 at 0x080490e8
(gdb) run
Starting program: /home/baranovjora/work/arch-pc/lab09/lab9-3 argument 1 argument 2 argument\ 3

Breakpoint 1, 0x080490e8 in _start ()
(gdb) x/x $esp
0xffffd190: 0x00000006
(gdb)
0xffffd194: 0xffffd354
(gdb) x/s *(void**)($esp + 4)
0xffffd354: "/home/baranovjora/work/arch-pc/lab09/lab9-3"
(gdb) x/s *(void**)($esp + 8)
0xffffd380: "argument"
(gdb) x/s *(void**)($esp + 12)
0xffffd389: "1"
(gdb) x/s *(void**)($esp + 16)
0xffffd38b: "argument"
(gdb) x/s *(void**)($esp + 20)
0xffffd394: "2"
(gdb) x/s *(void**)($esp + 24)
0xffffd396: "argument 3"
(gdb) c
Continuing.
argument
1
argument
2
argument 3
[Inferior 1 (process 2218) exited normally]
(gdb)
```

Рис. 3.16: Вывод значения регистра

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

3.3 Задание для самостоятельной работы

Я переписал программу из лабораторной работы №8, чтобы вычислить значение функции $f(x)$ в виде подпрограммы.

```
baranovjora@georgy-pc: ~/work/arch-pc/lab09
GNU nano 4.8 task.asm
#include 'in_out.asm'
SECTION .data
msg db "Результат: ",0
fx: db 'f(x)= 2x+15',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 proc
add esi,eax

loop next

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

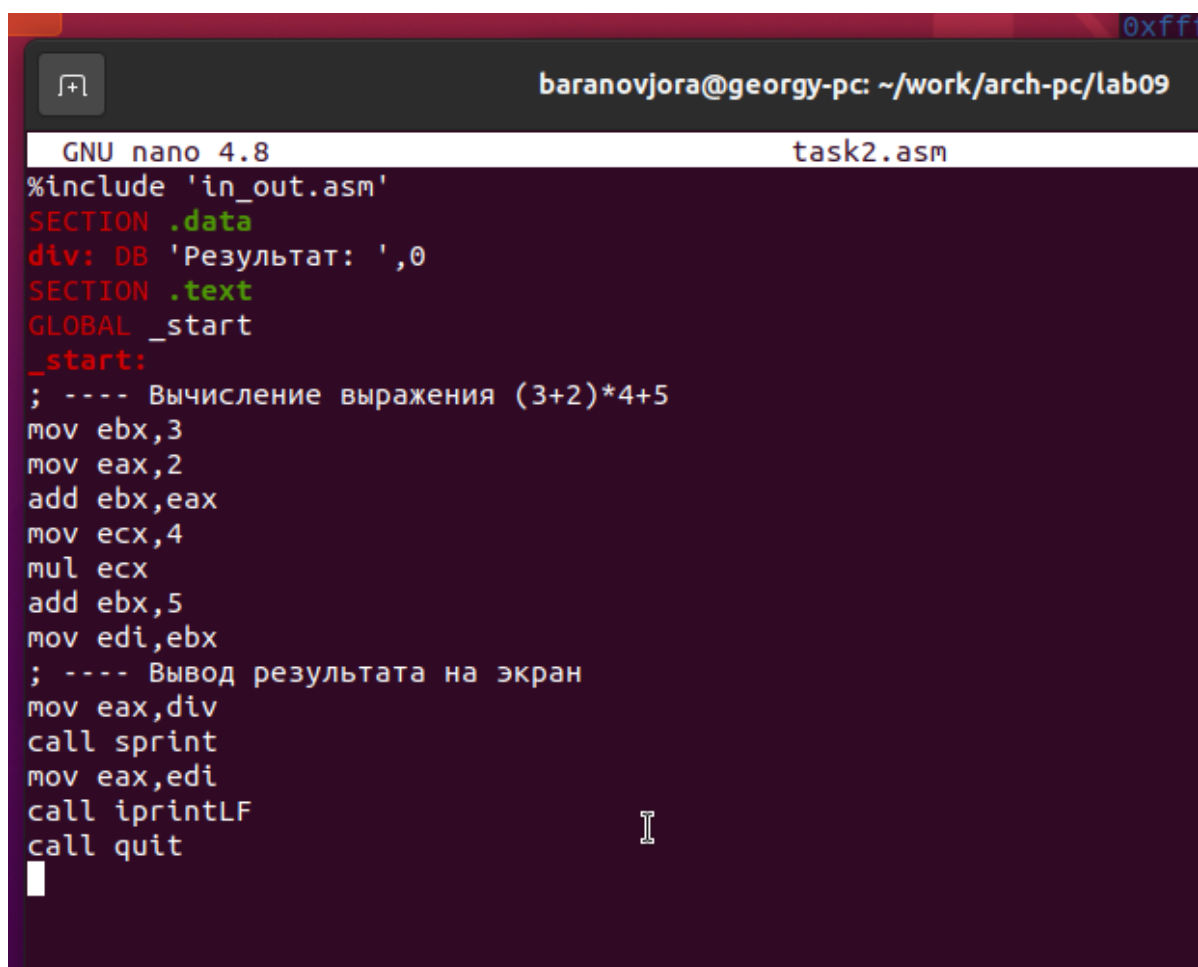
proc:
mov ebx,2
mul ebx
add eax,15
```

Рис. 3.17: Программа в файле task-1.asm

```
baranovjora@georgy-pc:~/work/arch-pc/lab09$  
baranovjora@georgy-pc:~/work/arch-pc/lab09$ nasm -f elf task.asm  
baranovjora@georgy-pc:~/work/arch-pc/lab09$ ld -m elf_i386 task.o -o task  
baranovjora@georgy-pc:~/work/arch-pc/lab09$ ./task 6  
f(x)= 2x+15  
Результат: 27  
baranovjora@georgy-pc:~/work/arch-pc/lab09$ ./task 9  
f(x)= 2x+15  
Результат: 33  
baranovjora@georgy-pc:~/work/arch-pc/lab09$ ./task 3 1 3 4 9 4  
f(x)= 2x+15  
Результат: 138  
baranovjora@georgy-pc:~/work/arch-pc/lab09$
```

Рис. 3.18: Запуск программы task-1.asm

Приведенный ниже листинг программы вычисляет выражение $(3 + 2) * 4 + 5$. Однако, при запуске, программа дает неверный результат. Я проверил это и решил использовать отладчик GDB для анализа изменений значений регистров и определения ошибки.



The screenshot shows a terminal window with a dark background. At the top, a status bar displays the username and path: `baranovjora@georgy-pc: ~/work/arch-pc/lab09`. Below this, the editor title bar shows `GNU nano 4.8` and the filename `task2.asm`. The main area contains assembly code. The code starts with `%include 'in_out.asm'`, followed by a data section `SECTION .data` containing `div: DB 'Результат: ',0`. Then, a text section `SECTION .text` begins with `GLOBAL _start`. The `_start:` label is followed by a comment `; ---- Вычисление выражения (3+2)*4+5` and several instructions: `mov ebx,3`, `mov eax,2`, `add ebx,eax`, `mov ecx,4`, `mul ecx`, `add ebx,5`, and `mov edi,ebx`. Another comment `; ---- Вывод результата на экран` is followed by `mov eax,div`, `call sprint`, `mov eax,edi`, `call iprintLF`, and `call quit`. The code ends with a blank line. A cursor is visible on the line `call iprintLF`.

```
%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. 3.19: Код с ошибкой в файле task-2.asm

```

baranovjora@georgy-pc: ~/work/arch-pc/lab09

eax      0x8      8
ecx      0x4      4
edx      0x0      0
ebx      0xa      10
esp      0xffffd1d0 0xffffd1d0
ebp      0x0      0x0
esi      0x0      0
edi      0x0      0
eip      0x80490fe 0x80490fe <_start+22>
eflags   0x206    [ PF IF ]
cs       0x23     35
ss       0x2b     43

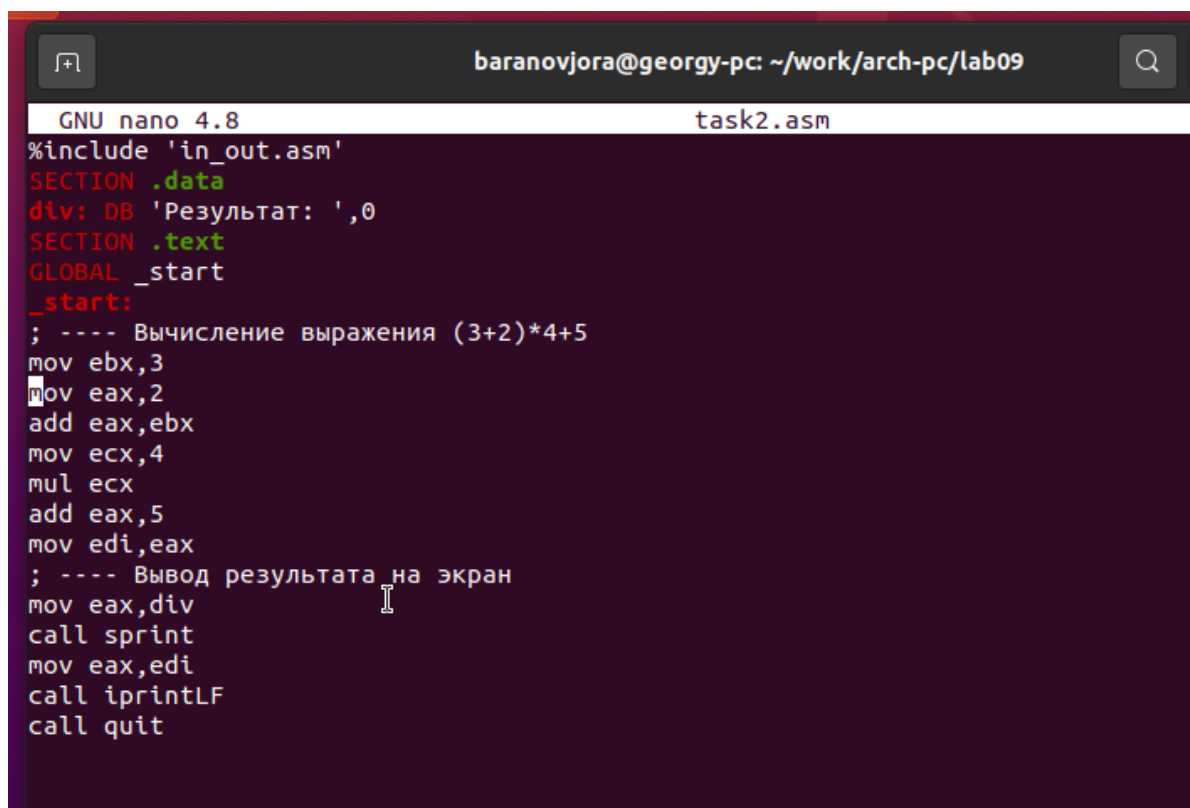
B+ 0x80490e8 <_start>    mov     ebx,0x3
B+ 0x80490e8 <_start+5>   mov     ebx,0x3
0x80490ed <_start+5>     mov     eax,0x2
0x80490f2 <_start+10>    add     ebx,eax
0x80490f4 <_start+12>    mov     ecx,0x4
0x80490f9 <_start+17>    mul     ecx,0x5
>0x80490fb <_start+19>    add     ebx,0x5
0x80490fe <_start+22>    mov     edi,ebx
0x8049100 <_start+24>    mov     eax,0x804a000<rint>
0x8049105 <_start+29>    call   0x804900f <sprint>
0x804910a <_start+34>    mov     eax,edi86 <iprintLF>
0x804910c <_start+36>    call   0x8049086 <iprintLF>
0x8049111 <_start+41>    call   0x80490db <quit>

native process 2273 In: _start L?? PC: 0x80490fe
(gdb) sNo process In: L?? PC: ??
(gdb) si
0x80490f4 in _start ()
(gdb) si
0x80490f9 in _start ()
(gdb) si
0x80490fb in _start ()
(gdb) si
0x80490fe in _start ()
(gdb) c
Continuing.
Результат: 10
[Inferior 1 (process 2273) exited normally]
(gdb)

```

Рис. 3.20: Отладка task-2.asm

Я заметил, что порядок аргументов в инструкции add был перепутан и что при завершении работы, вместо eax, значение отправлялось в edi. Вот исправленный код программы:



```
baranovjora@georgy-pc: ~/work/arch-pc/lab09
GNU nano 4.8 task2.asm
#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. 3.21: Код исправлен в файле task-2.asm

```
baranovjora@georgy-pc: ~/work/arch-pc/lab09

eax      0x19      25
ecx      0x4       4
edx      0x0       0
ebx      0x3       3
esp      0xffffd1d0 0xffffd1d0
ebp      0x0       0x0
esi      0x0       0
edi      0x0       0
eip      0x80490fe 0x80490fe <_start+22>
eflags   0x202     [ IF ]
cs       0x23      35
ss       0x2b      43

B+ 0x80490e8 <_start>    mov     ebx,0x3
B+ 0x80490e8 <_start>5>   mov     ebx,0x3
0x80490ed <_start+5>     mov     eax,0x2
0x80490f2 <_start+10>    add     eax,ebx
0x80490f4 <_start+12>    mov     ecx,0x4
0x80490f9 <_start+17>    mul     ecx,0x5
>0x80490fb <_start+19>    add     eax,0x5
0x80490fe <_start+22>    mov     edi,eax
0x8049100 <_start+24>    mov     eax,0x804a000rint>
0x8049105 <_start+29>    call   0x804900f <sprint>
0x804910a <_start+34>    mov     eax,edi86 <iprintLF>
0x804910c <_start+36>    call   0x8049086 <iprintLF>
0x8049111 <_start+41>    call   0x80490db <quit>

native process 2299 In: _start L?? PC: 0x80490fe
(gdb) sNo process In: L?? PC: ??
(gdb) si
0x080490f4 in _start ()
(gdb) si
0x080490f9 in _start ()
(gdb) si
0x080490fb in _start ()
(gdb) si
0x080490fe in _start ()
(gdb) c
Continuing.
Результат: 25
[Inferior 1 (process 2299) exited normally]
(gdb) █
```

Рис. 3.22: Проверка работы task-2.asm

4 Выводы

Освоили работу с подпрограммами и отладчиком.