LAB 04

I.Lý Thuyết

Bài 1:

Khi thực hiện lệnh RET (return), bộ vi xử lý sẽ thực hiện hai bước:

B1: Lấy giá trị 16-bit từ đỉnh của ngăn xếp và gán giá trị này cho con trỏ lệnh IP.

B2: Cập nhật thanh ghi SP để chỉ ra rằng dữ liệu đã được lấy từ ngăn xếp.

-Dữ liệu 16-bit tại đỉnh ngăn xếp được lưu trữ ở vị trí mà SP đang trỏ tới. Lúc này, SP = 0200h, và giá trị tại đỉnh ngăn xếp là 012Ah. Khi thực hiện lệnh RET:

- Giá trị 012Ah sẽ được lấy ra khỏi ngăn xếp và gán cho IP.

- Sau đó, con trỏ ngăn xếp SP sẽ được tăng lên 2 đơn vị để trỏ tới vị trí tiếp theo trong ngăn xếp.

-Do đó, sau khi thực hiện lệnh RET:

- IP = 012Ah

- SP = 0202h

-Tóm lại, giá trị sau lệnh RET là:

- IP = 012Ah

- SP = 0202h.

Bài 2:

1. Lệnh CALL PROC1:

-Lệnh CALL sẽ thực hiện hai nhiệm vụ:

+Đẩy địa chỉ của lệnh kế tiếp vào ngăn xếp (địa chỉ quay lại).

+Nhảy tới địa chỉ của thủ tục (PROC1).

-Địa chỉ của lệnh kế tiếp là lệnh MOV AX, BX, nằm ở địa chỉ 08FD:0203. Như vậy, CALL PROC1 sẽ đẩy giá trị 0203h (chính là giá trị IP của lệnh kế tiếp) lên ngăn xếp.

-CALL PROC1 sẽ nhảy tới địa chỉ của thủ tục PROC1 tại 08FD:0300, do đó:

* + IP sẽ được gán giá trị 0300h.
  + SP sẽ giảm đi 2 đơn vị vì địa chỉ quay lại (0203h) đã được đẩy lên ngăn xếp.

1. Lệnh RET trong PROC1:
   * Lệnh RET sẽ lấy giá trị từ đỉnh ngăn xếp (giá trị được đẩy vào khi thực hiện CALL) và gán nó cho con trỏ lệnh IP.
   * Giá trị IP sẽ trở về 0203h (địa chỉ của lệnh MOV AX, BX).
   * SP sẽ tăng thêm 2 đơn vị để bỏ qua giá trị đã lấy từ ngăn xếp.

-Kết quả cuối cùng:

-Sau lệnh CALL PROC1:

* IP = 0300h (địa chỉ của PROC1)
* SP = SP\_initial - 2 (do giá trị 0203h đã được đẩy lên ngăn xếp)

-Sau lệnh RET trong PROC1:

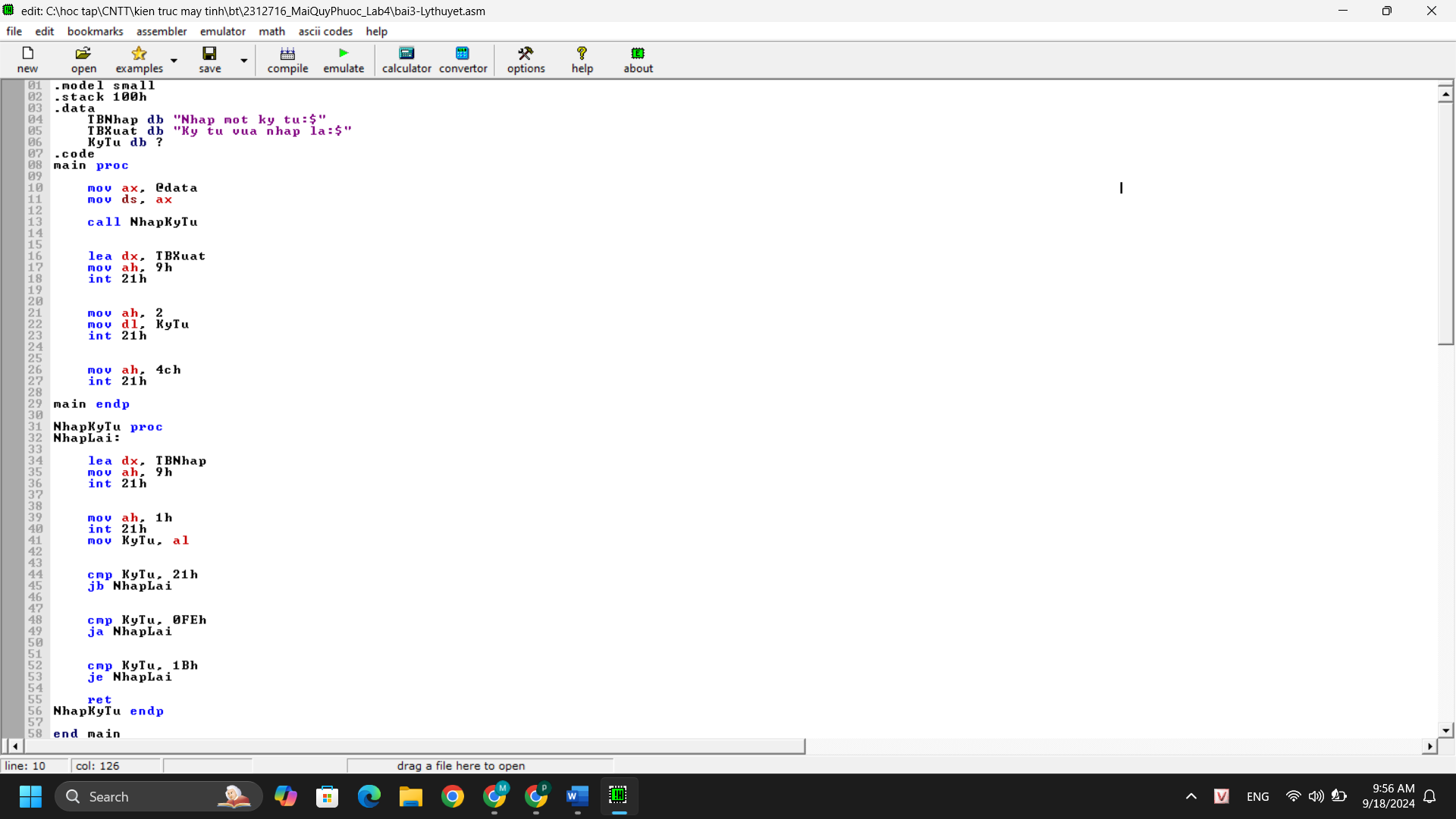
* IP = 0203h (quay lại lệnh MOV AX, BX)
* SP = SP\_initial (vì ngăn xếp đã được giải phóng sau khi RET).

-Nếu giả sử giá trị ban đầu của SP là 0200h, thì sau CALL PROC1:

* SP = 01FEh

-Và sau lệnh RET, SP quay lại 0200h.

Bài 3:



II.Bài Tập

1.