Tema 1 Subrutinas

Preparación y llamada
C:
a = foo(1,2)

ASM:
push 2
push 1 (los argumentos siempre se guardan en la pila)
call foo (guarda en la pila la @ de ret)

Dentro de la subrutina

```
int foo(int p1, int p2)
{
   push ebp  (guarda la @ donde estaba la base antes de llamar a la funcion
   mov ebp, esp  (dest, orig)  (ebp apunta a la base de la pila de subrut)
   subs esp, #vars  (reserva memoria para las variables locales)
   return p1+p2 (siempre devuelve en eax)
}
```

Los parametros se guardan de derecha a izquierda. el de mas a la derecha esta mas arriba en la pila. luego hace el call.

$esp apunta a lo mas alto de la pila, que son las posiciones más bajas

$ebp apunta a la base de la pila, no se mueve porque sirve como referencia.

Vuelve a la rutina

Limpia la pila de rutina

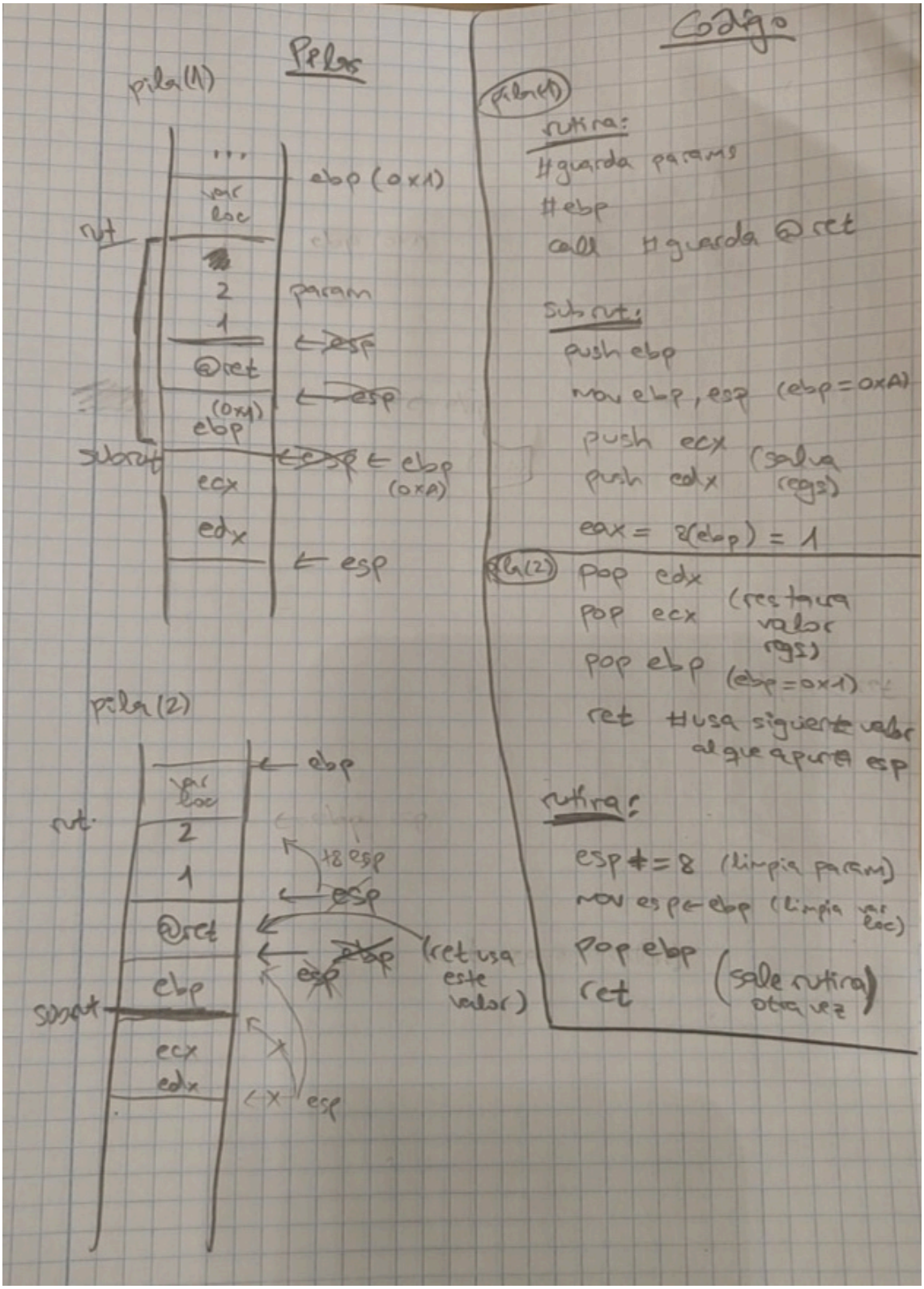
esp<-esp+8 (limpia los parametros de la pila)

Add esp, 8 (otra manera de limpiar la pila)

mov esp <- ebp (elimina las variables locales de la pila)

pop ebp (ebp vuelve a la base de la pila de rutina)

ret (vuelve a la @ contenida en ebp)



Convención C

- Los parámetros se guardan de derecha a izquierda
- Los vectores y matrices se pasan por referencia
- Los structs se pasan por valor
- Chars y Shorts no existen, se rellenan con 0's y son Enteros
- Los registros %ebx, %esi, %edi se han de guardar si se modifican
- Los registros %eax, %ecx y %edx se pueden modificar en una subrutina, por lo que se ha de guardar el valor en el código que llama a dicha subrutina, si es necesario.
- Los resultados siempre vuelven en %eax

Bloque de activación: la pila de usuario funciona con marcos de pila, son áreas de memoria reservada para ejecución de una rutina, se guardan los argumentos, la @ de retorno de las subrutinas, las variables locales, y registros salvados. Cada subrutina tiene su bloque de activación en la pila.

Argumentos: valores que se pasa a una función que se llama.
Parámetros: valores que recibe una función llamada.

Los argumentos se guardan en la pila. Cuando se llama a una subrutina, se guarda la @ de retorno de esta en la pila.

En cuanto se llama a la subrutina, EBP pasa a apuntar a la pila, pasando a ser igual a ESP, así, EBP se convierte en referencia base de los parámetros de la subrutina, por lo que se utiliza para acceder a estos.

ESP decrementa para reservar espacio en la pila, y aumenta para liberar, porque la pila crece hacia debajo.