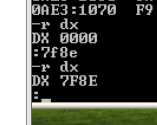


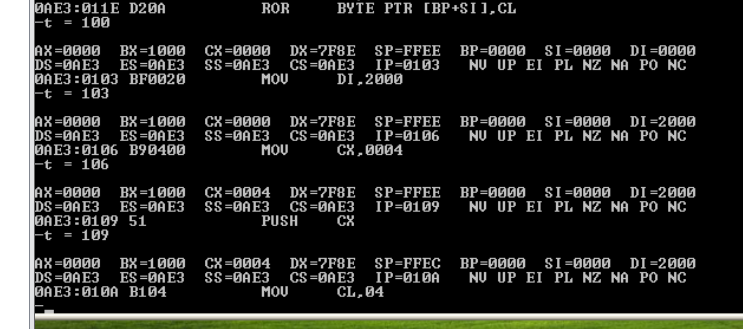
（2）

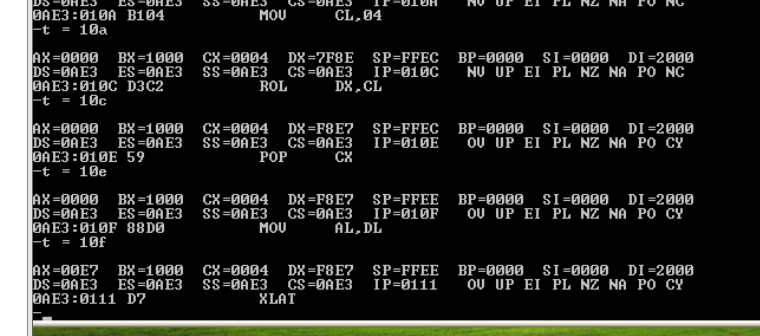


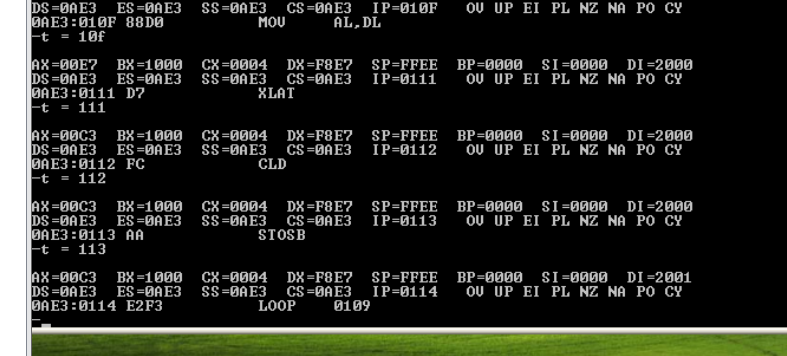
（3）



（4）

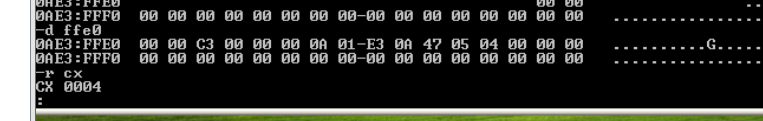






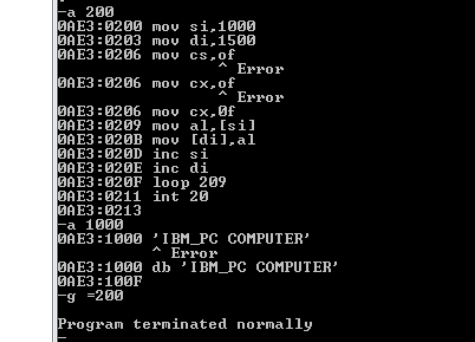
可以看到我们在执行pop和push操作时，sp寄存器进行了运算，push时ep指针会减2，pop指令相反

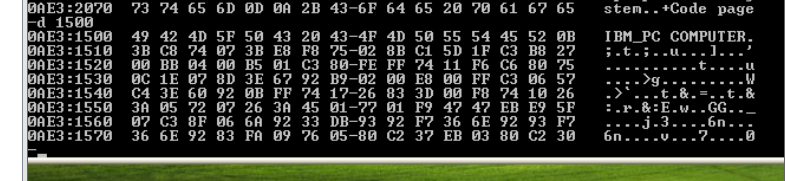
其中执行push cx时观察



恰好将其压到了ffec位置

3题





我们发现程序已经将字符串转移到了1500h位置