实验环境：

操作系统win10,编译器visual studio 2022,处理器Intel(R) Core(TM) i5-1035G1 CPU @ 1.00GHz   1.19 GHz

SM3的优化方法主要有：

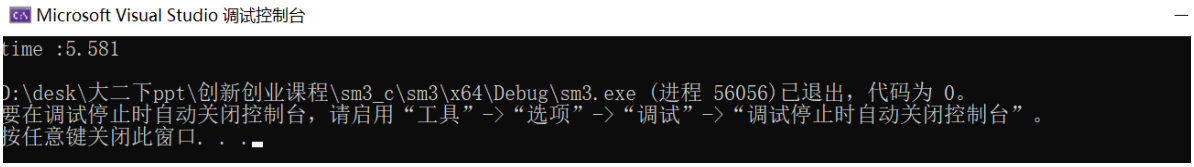
1、减少函数调用

2、尽量使用逻辑运算

3、使用simd指令集进行优化

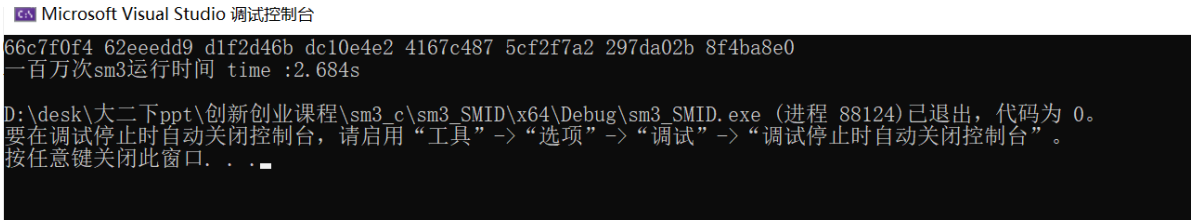
优化效果：

优化前：



进行一百万次sm3用时6s左右。

优化后：



进行一百万次sm3用时仅需3s,提速100%。