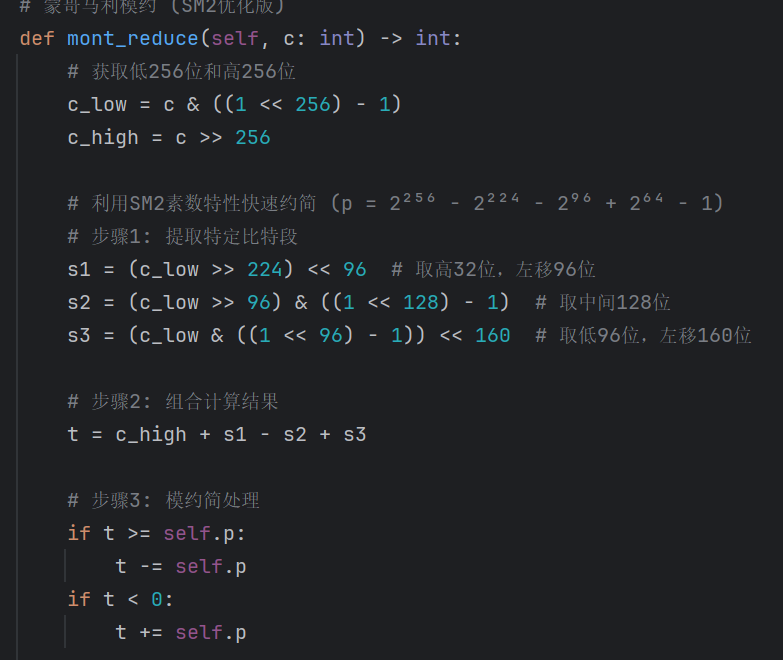
**任务5（poc推导文档）**

**1. 大数模约减优化（预计算表法）**

我们需要把大数乘法结果（512位）需约减到256位素域内，我们可以使用文档Page6里面的预计算表法。首先预计算表的存储如下：np[i] = i \* p（i=0..4），然后约减步骤为，先将512位结果拆分为高4位索引c和低256位b，之后计算b' = b - np[c]，最后若b'产生借位，则b' = b' + p。其中它的数学依据是，，利用预计算表避免实时计算**c\*p**。

代码如下图所示：



**2. 固定点点乘（kG）优化**

利用Page9里面的内容优化，Page9里面使用了预计算表+比特分组，其中预计算表为存储T[i] = (i+1) \* G（i=0..255），分组方法为将k按比特位拆分为32组kb[0..31]（每组8位），最后在使用点乘算法。Poc的验证代码如下图所示：

文本

AI 生成的内容可能不正确。

**3. 非固定点点乘（kP）优化（NAF编码）**

使用文档Page 11里面的内容优化，先将标量**k**编码为无连续非零比特的形式，然后当窗口宽度w=5时，使得非零元素降至42个

然后进行预计算，存储奇数倍点 {P, 3P, 5P, ..., (2^{w-1}-1)P}。最后在使用点乘算法，代码的具体内容如下图所示：

文本

AI 生成的内容可能不正确。