## **第9章 SM9标识密码算法**

**1．设G1、G2是加法群，GT是乘法群，阶n=15，现有P1∈G1，P2∈G2，Q∈G2，并且Q=[5]P2，已知e(P1,P2)=2，求e([4](P1,Q))。**

解：由双线性对的双线性特性可知

e([4](P1,Q))= e([4]P1,[5]P2))=e(P1,P2)5×4=e (P1,P2)20=220(mod15)=1

**2．在SM9加密和解密算法中，C3=MAC(K2,C2),u=MAC(,C2),证明u=C3。**

解：在加解密流程中，，，证明u=C3成功的关键是与是否相等。而根据相关步骤可知，，，、分别为K和K’中的一部分，因此证明与相等即可。

在加密算法中，，而，根据双线性对的相关性质可得





而在解密算法中



因此：

