《离散数学二》第一次作业

1. 分别计算下面四个模算术公式值，写出具体过程：

(177 **mod** 31 ⋅ 270 **mod** 31) **mod** 31

(212 **mod** 15)3 **mod** 22

12100 **mod** 5

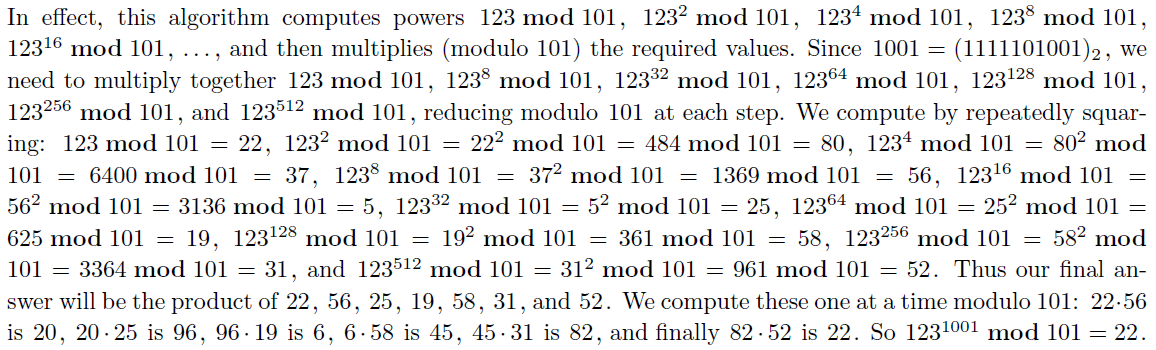
1231001 **mod** 101 (提示：用二进制模幂计算算法)

参考答案：





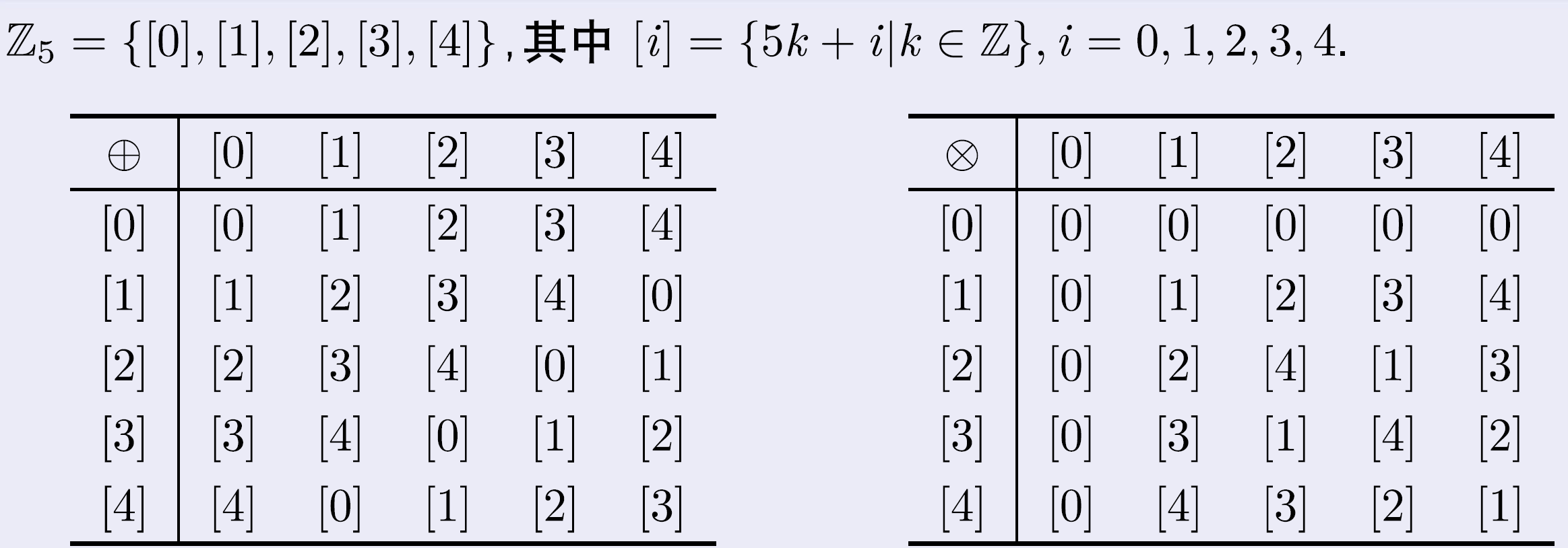
12^100 mod 5= 2^100 mod 5=16^25 mod 5=1^25 mod 5=1



1. （1）在Z5中编写加法和乘法表（这里的加法和乘法指的是模5加法和模5乘法）；（2）从你所写加法和乘法表中看，集合Z5及其模5加法是否满足封闭性、结合律和交换律？是否存在该加法单位元？如有，请写出该单位元。集合中每个元素是否存在加法逆元？如有，请写出集合中每个元素的加法逆元；（3）集合Z5及其模5乘法是否满足封闭性、结合律和交换律？是否存在该乘法单位元？如有，请写出该单位元。集合中每个元素是否存在乘法逆元（0元素除外）？如有，请写出集合中每个元素的乘法逆元（0元素除外）；（4）请验证该集合Z5以及其上的两个二元运算（模5加法和模5乘法是否构成整环？是否构成有限域？

参考答案：

（1）（下列两表中数字外的中括号可删去）



（2）均满足，加法单位元0,其中0,1,2,3,4的加法逆元分别是0,4,3,2,1；

（3）均满足，乘法单位元1,其中1,2,3,4的乘法逆元分别是1,3,2,4；

（4）构成整环，因为加法为阿贝尔群，乘法满足封闭、结合、交换律，存在乘法单位元，没有零因子（两个非零元素乘结果为零），且乘法对加法满足分配律；构成有限域，因为集合有限，为整环且非0元素存在乘法逆元（0元素除外）。

1. 用扩展欧几里得算法把 gcd(100001, 1001) 表示成 100001和1001的线性组合。

参考答案：

