

## 《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, 写具体过程(前两题每题 **5** 分, 后两题每题 **10** 分) :

(1)  $(177 \bmod 31 \cdot 270 \bmod 31) \bmod 31$

(2)  $(21^2 \bmod 15)^3 \bmod 22$

(3)  $12^{100} \bmod 5$

(4)  $123^{1001} \bmod 101$  (提示: 用二进制模幂计算算法)

2. 在  $Z_5$  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); [10 分] (2) 从你所写加法和乘法表中看, 集合  $Z_5$  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; [15 分] (3) 集合  $Z_5$  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); [15 分]

3. 用扩展欧几里得算法把  $\gcd(100001, 1001)$  表示成 100001 和 1001 的线性组合, 要求写出具体计算过程。[30 分]