《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

$(21^2$ **mod** $15)^3$ **mod** 22

12^{100} **mod** 5

123^{1001} **mod** 101 (提示：用二进制模幂计算算法)

参考答案：

$$(177 \mathbf{\ mod\ } 31 \cdot 270 \mathbf{\ mod\ } 31) \mathbf{\ mod\ } 31 = (22 \cdot 22) \mathbf{\ mod\ } 31 = 484 \mathbf{\ mod\ } 31 = 19$$

$$(21^2 \mathbf{\ mod\ } 15)^3 \mathbf{\ mod\ } 22 = (441 \mathbf{\ mod\ } 15)^3 \mathbf{\ mod\ } 22 = 6^3 \mathbf{\ mod\ } 22 = 216 \mathbf{\ mod\ } 22 = 18$$

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

In effect, this algorithm computes powers $123 \mathbf{\ mod\ } 101$, $123^2 \mathbf{\ mod\ } 101$, $123^4 \mathbf{\ mod\ } 101$, $123^8 \mathbf{\ mod\ } 101$, $123^{16} \mathbf{\ mod\ } 101, \ldots$, and then multiplies (modulo 101) the required values. Since $1001 = (1111101001)_2$, we need to multiply together $123 \mathbf{\ mod\ } 101$, $123^8 \mathbf{\ mod\ } 101$, $123^{32} \mathbf{\ mod\ } 101$, $123^{64} \mathbf{\ mod\ } 101$, $123^{128} \mathbf{\ mod\ } 101$, $123^{256} \mathbf{\ mod\ } 101$, and $123^{512} \mathbf{\ mod\ } 101$, reducing modulo 101 at each step. We compute by repeatedly squaring: $123 \mathbf{\ mod\ } 101 = 22$, $123^2 \mathbf{\ mod\ } 101 = 22^2 \mathbf{\ mod\ } 101 = 484 \mathbf{\ mod\ } 101 = 80$, $123^4 \mathbf{\ mod\ } 101 = 80^2 \mathbf{\ mod\ } 101 = 6400 \mathbf{\ mod\ } 101 = 37$, $123^8 \mathbf{\ mod\ } 101 = 37^2 \mathbf{\ mod\ } 101 = 1369 \mathbf{\ mod\ } 101 = 56$, $123^{16} \mathbf{\ mod\ } 101 = 56^2 \mathbf{\ mod\ } 101 = 3136 \mathbf{\ mod\ } 101 = 5$, $123^{32} \mathbf{\ mod\ } 101 = 5^2 \mathbf{\ mod\ } 101 = 25$, $123^{64} \mathbf{\ mod\ } 101 = 25^2 \mathbf{\ mod\ } 101 = 625 \mathbf{\ mod\ } 101 = 19$, $123^{128} \mathbf{\ mod\ } 101 = 19^2 \mathbf{\ mod\ } 101 = 361 \mathbf{\ mod\ } 101 = 58$, $123^{256} \mathbf{\ mod\ } 101 = 58^2 \mathbf{\ mod\ } 101 = 3364 \mathbf{\ mod\ } 101 = 31$, and $123^{512} \mathbf{\ mod\ } 101 = 31^2 \mathbf{\ mod\ } 101 = 961 \mathbf{\ mod\ } 101 = 52$. Thus our final answer will be the product of 22, 56, 25, 19, 58, 31, and 52. We compute these one at a time modulo 101: $22 \cdot 56$ is 20, $20 \cdot 25$ is 96, $96 \cdot 19$ is 6, $6 \cdot 58$ is 45, $45 \cdot 31$ is 82, and finally $82 \cdot 52$ is 22. So $123^{1001} \mathbf{\ mod\ } 101 = 22$.

2. （1）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）；（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；（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）；（4）请验证该集合 Z_5 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）

$\mathbb{Z}_5 = \{[0],[1],[2],[3],[4]\}$，其中 $[i] = \{5k+i \mid k \in \mathbb{Z}\}, i = 0,1,2,3,4.$

$\oplus$	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]	[0]
[2]	[2]	[3]	[4]	[0]	[1]
[3]	[3]	[4]	[0]	[1]	[2]
[4]	[4]	[0]	[1]	[2]	[3]

$\otimes$	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]
[2]	[0]	[2]	[4]	[1]	[3]
[3]	[0]	[3]	[1]	[4]	[2]
[4]	[0]	[4]	[3]	[2]	[1]

（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）。

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。

参考答案:

We take $a = 100001$ and $b = 1001$ to avoid a needless first step. When we apply the Euclidean algorithm we obtain the following quotients and remainders: $q_1 = 99$, $r_2 = 902$, $q_2 = 1$, $r_3 = 99$, $q_3 = 9$, $r_4 = 11$, $q_4 = 9$. Note that $n = 4$. Thus we compute the successive s's and t's as follows, using the given recurrences:

$s_2 = s_0 - q_1 s_1 = 1 - 99 \cdot 0 = 1,$ $\qquad t_2 = t_0 - q_1 t_1 = 0 - 99 \cdot 1 = -99$

$s_3 = s_1 - q_2 s_2 = 0 - 1 \cdot 1 = -1,$ $\qquad t_3 = t_1 - q_2 t_2 = 1 - 1 \cdot (-99) = 100$

$s_4 = s_2 - q_3 s_3 = 1 - 9 \cdot (-1) = 10,$ $\qquad t_4 = t_2 - q_3 t_3 = -99 - 9 \cdot 100 = -999$

Thus we have $s_4 a + t_4 b = 10 \cdot 100001 + (-999) \cdot 1001 = 11$, which is $\gcd(100001, 1001)$.