华中科技大学计算机与科学技术学院 2024~2025 第一学期

“ 离散数学（二） ”期中考试试卷

考试方式 闭卷 考试日期 2024-10-16 考试时长 50 分钟

专业班级 ______ 学 号 ______ 姓 名 ______

题号	1	2	3	4	5	6	7	总分	总分人	核对人
分值	20	10	10	20	10	10	20	100		
得分										

解答内容不得超过装订线

1. 分别计算 3^{963} mod 35 以及 17! mod 19 的值。（20 分）

参考答案：因为 gcd(3,35)=1，且 φ(35)=24，则 3^{963} mod 35=3^3 mod 35=27；因为 19 为质数，先计算 18 mod 19 的逆元为-1，再在 18! (mod 19)=-1 (mod 19)两端同时乘上 18 mod 19 的逆元，即-1，可得 17! (mod 19)=1 (mod 19)

2. 求线性同余式 35x≡10 mod 50 的所有解。（10 分）

参考答案：化简上述同余式得 7x≡2 mod 10，再求 7 mod 10 的逆元为 3，因此 x≡6 mod 10，即 x=6+10k，这里 k 是任意整数，即 x=6,16,26,36,…, -4,-14,-24,…。

3. 将整数 5 允许重复地有序拆分成三个非负整数的方案有几个？要求写出具体求解过程。（10 分）

参考答案：即求 x1+x2+x3=5，其中 x1, x2 和 x3 均为非负整数的解个数，允许重复的组合，即 C(3+5-1,2)=C(7,2)=21 个方案。具体如下：(5,0,0),(0,5,0),(0,0,5)，（4,1,0），（4,0,1），（1,4,0），（1,0,4），（0,4,1），（0,1,4），（3,2,0），（3,0,2），（2,3,0），（2,0,3），（0,3,2），（0,2,3），（3,1,1），（1,3,1），（1,1,3），（2,2,1），（2,1,2），（1,2,2）；

4. 某班有 7 个男同学，6 个女同学，现要组织一个由数目为奇数的男同学和数目不少于 3 的女同学组成的小组，问选 11 人多少种组成方式？要求分别给出所选男女同学的离散序列和相应生成函数再进行求解。(20 分)

参考答案：令 a_n 为从 7 位男同学中抽取出 n 个的允许组合数。由于要求其数目必须是奇数。故 $a_1=C(7,1)=7, a_3=C(7,3)=35, a_5=C(7,5)=21, a_7=C(7,7)=1, a_0=a_2=a_4=a_6=0$，其生成函数 $A(x)=7x+35x^3+21x^5+x^7$。令 b_n 为从 6 位女同学中抽取出 n 个的允许组合数。由于要求其数目大于或等于 3。故 $b_0= b_1=b_2=0, b_3=C(6,3)=20, b_4=C(6,4)=15, b_5=C(6,5)=6, b_6=C(6,6)=1$，其生成函数 $B(x)= 20x^3+15x^4+6x^5+x^6$。求 $A(x)*B(x)$中 x^{11} 系数为 36。
$A(x)*B(x)= x^{13}+6x^{12}+36x^{11}+146x^{10}+350x^9+630x^8+532x^7+742x^6+105x^5+140x^4$。这题只要正确求出 x^{11} 系数即可。

5. 3 个有区别的球放进 4 个有标志的盒子里，要求 1，2 两个盒子必须有奇数个球，第 3 个盒子有偶数个球，求不同的方案个数，并列出。[提示：可用指数型生成函数求解]（10 分）

参考答案：题目相当于把 1,2,3,4 允许重复地排成三位数的个数，要求 1 和 2 出现的次数为奇数，3 出现的次数为偶数，4 出现的次序不限。例如数字 124，其中第 i 位的数字表示把第 i 个球放到标号为该数字的盒子里，这里 124 相当于把第 1 个球放到盒子 1，第二个球放到盒子 2，第三个球放到盒子 4。

因为要求 1 和 2 出现的次数为奇数，最多为 3 次，因此其指数型生成函数 $A(x)=(x+x^3/3!)^2$，因为要求 3 出现的次数为偶数，最多为 2 次，因此其指数型生成函数 $B(x)=(1+ x^2/2!)$，因为 4 出现的次数不限，最多 3 次，因此其指数型生成函数 $C(x)=(1+x+x^2/2!+x^3/3!)$。求 $A(x)*B(x)*C(x)$的展开式中 $x^3/3!$ 的系数为 6，因此有 6 种，分别为 124,142,214,241,412

和421。这里3均出现0次，表示没有任何球扔到盒子3中。

6. 证明：当p是质数且e是正整数时，欧拉函数$\varphi(p^e)=p^{e-1}(p-1)$，这里欧拉函数$\varphi(n)$表示小于或等于n的正整数中与n互质的数的个数。(10分)

参考答案：与p^e不互质的数有p,2p,3p,4p,…p^e ，这里最后一个数p^e可以表示成$p^{e-1}*p$，所以共有p^{e-1}个数与p^e不互质；此外小于或等于p^e的正整数有p^e个，因此$\varphi(p^e)= p^e - p^{e-1}= p^{e-1}(p-1)$，举例而言，$\varphi(8)= \varphi(2^3)=4*1=4$，即1,3,5,7四个数。

7. （1）Alice和Bob使用 Diffie-Hellman 密钥交换协议生成共享密钥，假设他们使用素数p=23，并取原根g=5，且Alice选择私钥a= 6，而 Bob 选择私钥 b=15，计算他们各自使用的公钥和共享密钥；（2）Alice拟用凯撒密码（即Shift Cipher）作为对称加密算法对字符串“HELLO”进行加密并发给Bob，然后Bob再用凯撒密码进行解密，分别写出Alice发送的密文和Bob解密的明文，写出过程，这里密钥即为各自的共享密钥。(20分）

参考答案：

（1）Alice计算其公钥为5ˆ6 mod 23=8，Bob计算其公钥为5ˆ15 mod 23=19，则Alice的共享密钥为 19ˆ6 mod 23=2，而Bob的共享密钥为8ˆ15 mod 23=2；

(2) 即f(p)=p+2，则Alice发送的密文为JGNNQ；而Bob则采用f(p)的逆函数p-2，则其解密的明文为HELLO。

解答内容不得超过装订线