“ 离散数学（二）”样板题解答

一. 填空题(每小题 4 分，共 24 分)

(1) 1---20 中至少要取__11_个数才能保证取到的数中一定有一个是另一个的因数。

解：1—20 中，11-20 这 10 个数是最大的不存在一个整除另一个的情况。再添加任意的一个数进入，都必然存在一个整除另一个。这道题错的人比较多

(2) 9 个人平均分成 3 部分有____280______种分法。

解：9 个人分成 3 份，每个部分是没有编号的。可以先给 3 份编个号，相当于 9 平均分到 3 个编号的组中。在每个组有编号的情况下，总的分配方案数是：C(9,3)C(6,3). 由于组是没有编号的，所以上面这个方案数里面都有重复，重复次数为 P(3,3)=3!，所以答案是 C(9,3)C(6,3)/6 = 280

(3) 三元四次多项式最多有_____15 或 35_____项。

解：这道题没有注明是齐次还是非齐次，所以无论是计算齐次的还是非齐次的都算正确。按齐次的算是 15（齐 4 次）；再加上 3 次，2 次，1 次以及 0 次的，最多是 35。

(4) 10 个人举行一次舞会，其中 3 个女生，7 个男生，规定女生不可能跟女生跳舞，每个人都必须找一个舞伴跳舞，共有____630______种舞伴的搭配方案。

解：由于女生不能跟女生跳舞，所以 3 个女生需要从 7 个男生里面任选 3 个出来搭配跳舞，这有 P(7,3)中搭配方案；剩下的 4 个男生有 3 种搭配方案。根据乘法原理，得到一共有 3P(7,3) = 630 种方案。

(5) 10 个一样的苹果分配给 4 个孩子吃，每个孩子都必须分到苹果。共有____84____

解答内容不得超过装订线

种分配方案。

解答：由于每个人都必须分配到苹果，相当于 6 个苹果分配给 4 个人，不加限制的方案数。 这就直接用可重复组合数的公式：C(6+4-1, 4-1)=84.

(6) 7 模 10 的逆是____3+10k (k 为整数)____.

当然，这里只写一个 3 也给满分。

分 数	
评卷人	

二． 解答题（共 46 分）

(7) 不含有两个连续 1 的 n 位的二进制串有多少个？要求写出一个递推关系，以及递推关系的初始条件。(6 分)

解法 1：这道题可以直接做。假设满足条件的 n 位二进制串的个数为 a_n.

当 $n\geqslant 2$ 时， 如果第 1 为为 0，那么满足条件的串的个数就是 a_{n-1};

如果第 1 位为 1， 那么第 2 位一定不能是 1， 只能是 0，否则就已经有连续 1 了；这种情况的个数为 a_{n-2};

所以 $a_n = a_{n-1} + a_{n-2}, n\geqslant 2$. C 初始条件为：$a_0=1, a_1 = 2, a_2 = 3$. 当然，初始条件就写前面两个，或者后面两个，或者前面 3 个度可以。 但是，递推关系式后面的“$n\geqslant 2$”是需要的。 这就是斐波那契 Fibonacci 序列。

解法 2： 也可以是求出含有两个连续 1 的串的个数，然后，再用总数 2^n 减去这个数字，结果跟上面一样。

这道题跟平时做的作业题基本相同，没有什么难度。比去年考题简单多了。

(8) 解递推式：$a_n = 5a_{n-1} - 4a_{n-2} - 9n^2 + 15n - 3, n \geq 4$. 已知 $a_2 = 11, a_3 = 0$. (10 分)

解析：这道题的正常的做法的步骤是：

(1) 写出相伴的齐次递推关系的特征方程，求出两个特征根 r=1 与 r=4；

(2) 写出相比齐次递推关系的通解的形式；

(3) 由于该递推关系的非齐次部分为一个 2 次多项式，试探 2 次多项式形式的特解，本题无解。 再试探 3 次多项式形式的特解。

(4) 求出一个特解；

(5) 解的一般形式是 通解 + 特解

(6) 根据初始条件，求出最终解。

客观地说，这道题的运算量有些大，容易计算错误。这一点，出题时系数搭配不太好，很多同学计算错误。

但只要其它都正确，只是计算特解以及后面计算出错，仅仅扣除 2 分。

但是，上面的求解过程，尤其是求齐次递推关系、通解形式、最终解的形式等，都是基本要求。还是不少人不会做，这就没有办法了。

具体的答案如下图所示：

解答内容不得超过装订线

(8) $\lambda^2-5\lambda+4=0$

$\lambda_1=1,\ \lambda_2=4$

一个特解:

$a_n=n(an^2+bn+c)$

$$
\begin{aligned}
&a_n-5a_{n-1}+4a_{n-2}\\
=&a(n^3-5(n-1)^3+4(n-2)^3)\\
&+b(n^2-5(n-1)^2+4(n-2)^2)\\
&+c(n-5(n-1)+4(n-2))\\
=&-9n^2+15n-3
\end{aligned}
$$

$$
\begin{cases}-27a+11b-3c=-3\\ -3a+5b-3c=3\\ 3a-b-3c=-9\end{cases}
$$

$$
\begin{cases}a=1\\ b=3\\ c=3\end{cases}
$$

通解:

$a_n=n^3+3n^2+3n+d+e\cdot 4^n$

代入 $a_2=11$. $a_3=0$ 得

$$
\begin{cases}26+d+16e=11\\ 63+d+64e=0\end{cases}
$$

$$
\begin{cases}d=1\\ e=-1\end{cases}
$$

故

$$
\begin{aligned}
a_n&=n^3+3n^2+3n+1-4^n\\
&=(n+1)^3-4^n
\end{aligned}
$$

(9) 用生成函数法，求方程 $x + y + z = 12$ 满足 $1\le x \le 4$, $2\le y \le 5$, $3\le z \le 6$ 的整数解的个数。(8 分)

解：生成函数 $G(X) = (X^1+X^2+X^3+X^4)(X^2+X^3+X^4+X^5)(X^3+X^4+X^5+X^6)$

$=X^6(1-X^4)^3/(1-X)^3$

该函数的展开式的 x^{12} 的系数即为所求，答案为 10。

这道题只要写出了正确的生成函数, 正确的答案就给满分了。无论展开过程是否详细写出来。

这道题是基本要求，不需要多少技巧，得分率也很高，部分同学的错误主要出现在以下 3 个方面 1. 写出了正确的生成函数，但展开过程出错，得到了错误的结果。
2. 没有按照题目要求使用生成函数法解决问题，如使用了穷举法等其他方法。
3. 生成函数写错了

解答内容不得超过装订线

(10) A,B,C,D,E,F,G,H 等 8 人参加体能考核，已知考核出了 3 种结果（优，及格，不及格），而且知道 B 的考核结果是优。 试问有多少种可能的结果搭配组合? (10 分)

解析：这道题看起来复杂，但计算量和难度都没有比去年的大。也就是容斥原理的基本应用。这里我给出两种解法如下：

由于 B 的考核结果已经定位优， 那么只考虑其他 7 个人的就是，而且其他 7 个人一定既要有 “及格 “又要有” 不及格 “，当然也可能出现” 优 “。

解法 1：假设用 p1 表示其他 7 个人没有出现 “及格 “，p2 表示其他 7 个人未出现” 不及格 “，N（¬p1¬p2）表示 7 个人种既要出现及格又要出现不及格的可能的组合数。 根据容斥原理，N（¬p1¬p2） $= 3^7 - [N(P1) + N(P2)] + N(P1P2)$

$= 3^7 - [2^7 + 2^7] + 1 = 1932$

其中， 3^7 的意义是 7 个元素到 3 个元素的函数的总个数， 2^7 的意义是 7 个人到两个元素的可能的函数的总个数（因为有一个结果取不到）。

解法 2： 可以采用分类的办法做。 B 的考核结果已定。 其他 7 个人中可能有人结果为优，也可能没有。 但是无论如何 7 个人一定要有结果及格和不及格。

所以，当 7 个人中有结果优时，可能的组合数相当于 7 个元素对 3 个元素的满射数量；

当 7 个人没有结果优时，相当于 7 个元素对 2 个元素的满射数量；

（求满射数量在学习容斥原理时学习过，也做过作业，去年的考题也是计算 8 个到 3 元素的满射的个数。）

再把上面两个数字求和，求和过程中可以抵消掉一些项，减轻计算量。最终结果还是一样， 1932.

最终答案是：1932

该题是考察容斥原理应用之映上函数个数问题。大部分的考生都能够正确作答。目前作答出现错误的考生的做题思路，整体而言大致分为以下几类问题：

1、出错中的大部分考生没有注意到题目中明确指出来的“已经出现 3 种考核结果”，因此大意的认为只需要考虑 7 个人，每个人有 3 种可能考核结果。导致他们认为该题只是在简单地考乘积法则，所以他们的结果为 3 的 7 次幂。
2、除以上第一种情况外，还有一小部分同学能够正确地写出所有的过程，但是最后一步的计算结果出错。
3、此外，还有小部分同学用生成函数来做该题。将题目变为 x1+x2+x3=7，然后 x1 限定为大于 0，x2 大于等于 1，x3 大于等 1。但本题中人是直接标明了 A,B,C,D,E,F,G,H 八个人，对应的结果是优，及格和不及格 3 种情况。所以该题不能这么求解。
4、还有一部分同学直接先将人分为三组，枚举出所有的情况，比如优有 4 人，及格有 1 人，不及格有 2 人。然后再用排名组合求解出每种情况下对应的数量有多少。该思路也是正确的，有同学通过该思想能够正确求解出答案。但部分同学虽然尝试枚举出所有的情况，但实际上没有把全部的可能出现的情况都一一罗列出来。导致最终答案不正确。
5、还有很少一部分同学，直接写了一个等式出来，结果又不对，没有任何解释如何求解该问题。

(11) 求 $(P^{17}-P+1)^{20} \bmod 12$，其中 P 是大于 3 的素数。(6 分)

解答：这道题是证明 12 整除$(P^{17}-P)$ 变化过来的。

$P^{17}-P = P(P^{16}-1)$

由于 P 是大于 3 的素数，所以必定跟 12 互素，也即 gcd(12, P)=1. 12 的欧拉函数值

$\Phi(12) = 4$ （这个作为欧拉函数值的定义的基本例题计算过）

所以根据费尔马小定理知 $P^4 \bmod 12 = 1$，于是 $P^{16} \bmod 12 = 1$. 那么（$P^{16}-1$）$\bmod 12 = 0$，也即$(P^{16}-1)$是 12 的倍数，那么 $P(P^{16}-1)$ 当然也是 12 的倍数。 于是 $(P^{17}-P+1)^{20} \bmod 12 = 1$

这道题计算简单，当然很多同学没有想到这些，没有动笔。

(12) 求解同余式：$35x \equiv 25 \pmod{76}$. (6 分)

解答：35 与模数 76 互素，也即 gcd(35, 76)=1

求得 35 关于模数 76 的模逆为-13 （或者 63）

用这个模逆同乘以同余方程的两边，得到

X = 55 mod76，所以得到方程解为： x= 55+ 76 k (k 为任意整数)。

错误分析：

这道题有同学不会动笔；

也有同学不会求模逆或者计算错误，求出了一个错的模逆；

求出模逆后不知道怎么做下去；

部分同学只求出了 55，没有写出通解。

解答内容不得超过装订线

三． 加解密题（共 10 分）

(13) 令 N=55, k=37, t=54. (10 分)

(a) 求出以 k 作为公钥，密文 t 对应的明文；

(b) 求出以 k 作为私钥，明文 t 对应的密文。

(c) 对于任意的两个不同的素数的乘积 n，假设不知道 RSA 算法使用的私钥。如果已知明文 M 以及相对应的密文 C，如何求出密钥？试给出求密钥的方程式。 并且分析求解该方程的可行性以及可能存在的问题。

解答：N=55=11*5， 所以其欧拉函数值 $\Phi(55) = 10*4 = 40$

(a) 当 k=37 作为公钥时，对应的私钥时 37 关于模 40 的模逆， 计算出该模逆

是 13. 于是这里 37 与 13 就是一对加解密的 key. 37 是公钥，那么 13 是私钥。于是这里的解密计算公式是 $54^{13} \bmod 55$，计算结果也是 54，于是从 54 解密还原的明文是 54。

(b) 当 k=37 作业私钥的时候, 13 就是公钥，由于明文 t=54，所以这里的加密计算公式是 $t^{13} \bmod 55 = 37^{13} \bmod 55 = 54$. (注：既然这个表达式跟 a 中表达式一样，当然计算结果也一定是一样的，就不需要再算一次。

(c) 明文为 M，密文为 C，模为 n，假设私钥为 x，那么从密文还原解密到明文的公式为 $C^{x} \bmod n = M$. 在这个表达式中，C,n, M 都已知，只有私钥 x 未知，这个就是一个计算私钥 x 的方程。 从这个方程中求解 x，就是求离散对数。 当模数 n 很大时，有限时间内几乎不可能。这也就是很难破解 RSA 算法的一个原因。

问题分析：

这道题是最基本的题目，明文密文设为 54， 模为 55 是为了计算简单。前面有题目计算量大，这道题计算量非常小。

1：直接用 37 作为指数求解，未求出 13。这就是没有搞清楚公钥私钥明文密文的意义及关系。也就是对整个 RSA 的过程不了解。这样得分就很低。

2：没有求出 55 的欧拉函数值 40，直接求 37 关于 55 的模逆。

3：一般来说，能求出 13 的同学，第一题一般都能全对，少数同学计算$54^{13} mod 55$错误，将结果写为了-1 或 1 或一些其他的数。

4：一些同学第一题用的 13 作为指数求解，但是第二题又用了 37 作为指数。

5：将$M = C^d mod\ \ n$写为了$C = M^e\ \ mod\ \ n$。也就是本来求密钥但是做成了求公钥。

6：得分率最高的是最后一小问，绝大多数都能写出来不好求。有些同学整道题就对了最后一小问，也有同学交的白卷。

分　数	
评卷人	

四. 证明题（每题 10 分，共 20 分）

(14)

问题分析：

解答内容不得超过装订线

(15) 用组合分析法证明：(10 分)

$$\sum_{k=0}^{m}\binom{n-k}{n-m}\binom{n}{k} = 2^m\binom{n}{m}$$

这道题也出乎意料，原以为这道题会有可能很多人做不出来，但结果还不错，得分率还比较高。

解题思路：用组合分析法证明这个恒等式，其实就是对同一个问题计数时，采用不同的方法，得到不同的表达式，最后说明是相等的。

问题解释（1） 从 n 对夫妻里面，选出 m 个人形成一个小组，但是每对夫妻都顶多只能选一个，不能夫妻同时都选上。
这种解释下，恒等式右边就是，先从 n 对夫妻里面选出 m 对，然后从这 m 对夫妻里每一对里面选一个人，每对夫妻选一个就有 2 种可能。 m 对就形成了 2m 可能，
再利用乘法原理，就得到了恒等式右边。
而左边， 利用这个 C(n-k, n-m) = C(n-k, m-k) 变一下，然后再证明。 变化后的，就是采取分类又分步的计数方法，和式里面的每一项，表示从 n 个里面先选 k 个男的出来，再在剩下没有被选的 m-k 对夫妻里面，选 m-k 个女的。
这样就可以完成了。

问题解释（2）可以想象 n 个带编号的围棋格子，放入颗围棋子， 围棋子就是黑白两

种选择。 有多少种可能的下法。
问题解释（3）n 个人，选出 m 个人去领奖，选出来的人有两种领奖的选择，红包或者礼品，但只能取一样。
还可以有很多种解释…，但计数的方法是类似的。