# 2021---2022 第一学期《离散数学二》试卷 (A 卷) 参考答案

(1) 一副扑克牌中 52 张（不包含大小王），至少要抽___40___张才能保证出 1 个炸弹（4 张牌同号）;

(2) $(a+b+c)^{10}$的展开式中$a^3b^2c^5$的系数是__2520__；

(3) 把 2n 个人分成 n 组，每组 2 人，有__$(2n)!/(2^n n!)$__分法;

(4) 10 个苹果分给 3 个小孩，每人至少一个，有__C(9, 2) = 36__种分发；

(5) $46^{550} \bmod 21$ = ____4____；

(6) 17 模 20 的逆是____13____.

(7) 问从 1, 4, 7,…, 3k+1, …, 100 中至少要取多少个数? 才能保证其中必有两数之和是 104. (6 分)

这些数分成 18 组：{1}, {52}, {4, 100}, …, {49, 55}，取 19 个数必有一组取两个。

这道题目也可以像如下这般处理一下再用鸽洞原理，显得更清晰：

序列中的每个数都是 3k+1 的形式；其中的任意两个不同的数之和可以假设为 3s+1 与 3t+1, 其中 0=<s<t<=33, 而且. 由于 s 为 0 的时候，1 与序列中任意一个数之和都不可能等于 104， 所以这里范围修改为 1<s<t<=33,问题转化为 1 到 33 这连续的 33 个整数，任取多少个能是的必有其中两个之和为 34. 这个答案是 18， 还需要把第一个数加进去，最终答案就是 19.

(8) 一个人爬阶梯，每次可以上 1 阶或 2 阶，求与爬 n 阶阶梯的方式数有关的递推关系和初始条件。(6 分)

$a_n = a_{n-1} + a_{n-2}$, $n \ge 2$. $a_0 = 1$, $a_1 = 1$.

(9) 解递推式：$a_n = 3a_{n-1} - 2a_{n-2} + 2 \cdot 3^n$, $n \ge 2$. 已知 $a_0 = 1$, $a_1 = 21$. (10 分)

$x^2 - 3x + 2 = (x - 1)(x - 2)$

有特解 $a3^n$，代入递推式得：$a = 9$

通解：$b + c2^n + 3^{n+2}$，代入初始值得：$b = -10$, $c = 2$

解为：$a_n = 3^{n+2} + 2^{n+1} - 10$

(10) 请用生成函数法，求方程 $x + y + z = 13$ 满足 $3 \le x \le 6, 3 \le y \le 6, 3 \le z \le 6$ 的整数解的个数。(8 分)

$(t^3 +\ldots+t^6)^3 = t^9(1 +\ldots+ t^3)^3 = t^9(1 - t^4)^3(1 - t)^{-3}$, $C(-3, 4) -3 = 12$

(11) A, B, C, D, E, F, G, H 等 8 人分成 3 组，要求 A, B 同组，C, D 不同组。问有多少种不同的分组方法? (10 分) （三个组不加区分）

{A, B 同组} 减去 {A, B 同组，C, D 同组}，即 7 到 3 的满射减去 6 到 3 的满射：$(3^7 - 3\bullet2^7 + 3) - (3^6 - 3\bullet2^6 + 3) = 2\bullet3^6 - 3\bullet2^6 = 6(3^5 - 2^5)$

三个组不加区分：$6(3^5 - 2^5)/6 = 3^5 - 2^5 = 243 - 32 = 211$

说明：这道题丢分的同学比较多。 绝大多数丢分的都是采用分类的方法，分成很多的类再求和。分类不清楚，有些重叠，有些有遗漏等错误导致得不到正确答案。。

(12) 求 9! 的正因数的个数。(6 分)

$9! = 2^7\bullet3^4\bullet5\bullet7$, 正因数个数: $8\times5\times2\times2 = 160$

(13) 求解同余式：$50x \equiv 15 \pmod{91}$. (6 分)

两边约去 5，$10x \equiv 3 \pmod{91}$，

$10\bullet9 \equiv -1 \pmod{91}$, $10\bullet(-27) \equiv 3 \pmod{91}$, $x \equiv -27 \equiv 64 \pmod{91}$

(14) 构造 RSA 公钥密码体系的密钥，令 N=91，(10 分)

(a) 以 d=31 为加密密钥，求对应的解密密钥 e;

(b) 求密文 45 对应的明文;

(c) 求明文 8 对应的密文。

$N = 91 = 7\times13$, $\phi(91) = 6\times12 =72$,

a) $31e \equiv 1 \pmod{72}$, $e \equiv 7 \pmod{72}$, $e = 7$.

b) $45^7\equiv 59 \pmod{91}$, 密文 45 对应的明文：59

c) $8^{31}\equiv 57 \pmod{91}$, 明文 8 对应的密文：57

说明：尽管这道题是标准题，而且没有任何技巧变化。但是也还是不少人丢分。有些同学用私钥加密，反而用公钥来解密；也有同学在加密和解密公式中，用 N=97 的欧拉函数值用于公司，不是用 N 求模余，导致基本公式用错。

(15) 证明：$3^{2n+2} - 8n - 9$ 能被 64 整除，其中$n \in \mathrm{N}$. (10 分)

令 m = n+1,

$3^{2n+2}-8n-9 = 9^m - 8m - 1 = (1+8)^m - 8m - 1 = 8^2C(m, 2) + 8^3C(m, 3) + \ldots$

说明：少数几个同学完全没有证明出来。 证明其能被 64 整除，在表达式的后面两个部分 -8n-9 中没有办法寻找出因子 64；只能从前面的 $3^{2n+2}$ 中去寻找，只要用一下二项式展开定理即可。

也可以用数学归纳法证明出来，也不难；

(16) 下式中 m, n, j 均为正整数，用组合分析法证明：(10 分)

$$\sum_{k=0}^{m}\binom{m}{k}\binom{n}{k+j}=\binom{m+n}{m+j}$$

右边表示：从 m+n 个不同的球中取出 m+j 个

左边：将球分成两堆，第一堆 m 个，第二堆 n 个。从第一堆取出 m – k 个，从第二堆取出 k + j 个，k = 0, 1, 2, …, m. 总的取法数即为左边的求和式。