

# “离散数学（二）”样卷

## 一. 判断与填空题

- (1) 表达式  $\exists z \forall x \forall y (x+y=z)$  (个体论域均为实数集) 的真值是\_\_\_\_\_.
- (2) 给定命题公式:  $(\neg P \rightarrow Q) \rightarrow (\neg P \wedge Q)$ , 该命题公式成真赋值的个数为\_\_\_\_\_.
- (3) 若将 10 个相同的球随机放入编号为 1, 2, 3 的三个盒子中, 每个盒子中小球个数不少于 1, 则有\_\_\_\_\_种放法:
- (4) 重新排列单词 MATHEMATICS 中的字母能构成\_\_\_\_\_个不同的串?
- (5) 从 1、2、3、4……、11、12 这 12 个自然数中, 至少任选\_\_\_\_\_个, 就可以保证其中一定包括两个数, 它们的差是 7.
- (6)  $27^{41}$  除以 77 所得余数是\_\_\_\_\_;
- (7)  $(x+2y-4z)^6$  展开式中  $x^3y^2z$  项的系数是\_\_\_\_\_.

## 二. 解答题

- (8) 求命题公式  $(P \rightarrow Q) \wedge (P \rightarrow R)$  的主合取范式 and 主析取范式.
- (9) 设  $B(x,y)$  为命题“y 是 x 最好的朋友”, 用谓词表达式将下列命题符号化:  
每个人有且仅有一个最好的朋友。
- (10) 判断下式是否成立, 如果成立, 说明理由, 如果不成立, 举例说明.  
$$\forall x (P(x) \rightarrow Q(x)) \Leftrightarrow \forall x P(x) \rightarrow \forall x Q(x)$$
- (11) 用扩展欧几里得算法把  $\gcd(1387, 162)$  表示成 1387 和 162 的线性组合.
- (12) 求满足下列同余式的  $x$ .  
$$26x \equiv 10 \pmod{62}$$

解答内容不得超过装订线

(13) 现有一长为  $n$  宽为 1 的地板，并有 4 种颜色的长宽均为 1 的瓷砖和 5 种颜色的长为 2 宽为 1 的瓷砖，设  $A_n$  为该地板的铺砖方案数，请给出  $A_n$  的递推式，并求初始值、通解以及  $A_6$  的值。

(14) 请用生成函数法，求方程  $x + y + z = 14$  满足  $1 \leq x \leq 8, 1 \leq y \leq 8, 1 \leq z \leq 8$  的整数解的个数。

(15) 6 本不同的书分给 4 个不同的学生，如果每个学生至少得到 1 本书，那么有多少种分法？

(16) 设 Alice 和 Bob 利用 RSA 公钥密码体系进行通信，Alice 的公钥:  $N_A=65, e_A=17$ ；Bob 的公钥  $N_B=77, e_B=13$ 。

(a) 分别求 Alice 和 Bob 的私钥  $d_A$  和  $d_B$ ；

(b) Alice 要把明文 23 加密发给 Bob，要求 Bob 知道这个消息为 Alice 所发并且只有 Bob 能够解密该消息，请写出具体过程计算 Alice 所发密文；[提示：Alice 用其私钥进行签名并用 Bob 公钥进行加密]

(c) 根据 Alice 所发密文，写出 Bob 解密过程和结果。[提示：Bob 用其私钥进行解密并用 Alice 公钥去除签名]。

### 三. 证明

(17) 证明若  $A \rightarrow (C \vee B), B \rightarrow \neg A$ ，则  $(D \rightarrow \neg C) \rightarrow (A \rightarrow \neg D)$ 。

(18) 已知  $p, q$  是两个不同的素数，且  $a^{p-1} \equiv 1 \pmod{q}$ ， $a^{q-1} \equiv 1 \pmod{p}$ 。

证明：  $a^{pq} \equiv a \pmod{pq}$

(19) 用生成函数证明  $\sum_{k=0}^m C(n+k, n) = C(n+m+1, n+1)$  其中  $m, n$  是非负整数