离散数学（二）”参考样卷

题号	一	二	三	四	五	六	总分	核对人
分值	14	62	24				100	
得分								

分　数	
评卷人	

一. 填空题(每小题 2 分，共 14 分)

(1) 表达式∃x∀y (xy=x+y) (个体论域均为实数集)的真值是____假____.

(2) 3 种不同的球中选取 5 个，可重复选取，有__21__种取法：

(3) 集合|A|=3，A 到 A 的满射 f 有_2_个满足：∀a∈A，f(a)≠a；

(4) 从 6 个元素（a1, a2 和 a3 各 2 个)中取 4 个元素的排列有_54__个；

(5) $3^{96} \equiv$ __21__ (mod 100)；

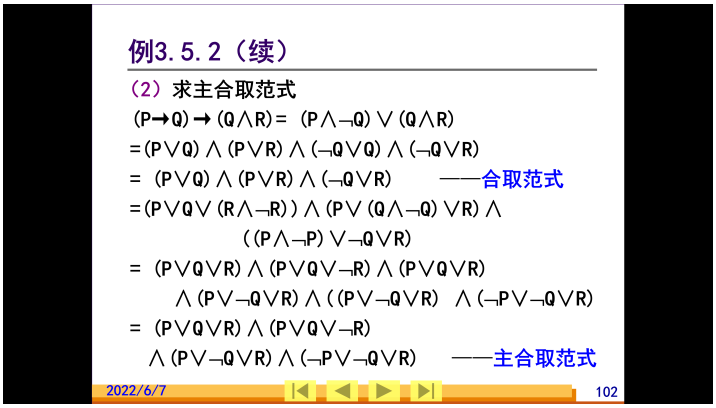
(6) 有__55_ 个没有连续“1”的 8 位二进制数。

(7) 以 2 为底，3 模 11 的离散对数是__8__。

分　数	
评卷人	

二. 解答题 （共 18 分）

(8) 求命题公式(P→Q)→(Q∧R)的主合取范式。(6 分)



(9) 用谓词表达式将下列命题符号化：(6 分)

没有一个男士接种过所有公司生产的某个疫苗。

P(x)：x 是男士。

V(x,y):x 接种了疫苗 y。

M(z,y):公司 z 生产的疫苗 y。

$\neg\exists x\,\exists y\forall z\,(P(x)\wedge V(x,y)\wedge M(z,y))$

(10)判断下式是否成立，并说明理由。(6 分)

$\forall x(P(x)\ \wedge\ Q(x)) \equiv \forall xP(x)\ \wedge\ \forall xQ(x)$

成立

设 A: $\forall x(P(x)\ \wedge\ Q(x))$；B：$\forall xP(x)\ \wedge\ \forall xQ(x)$

首先，A->B 的证明如下：

假设$\forall x(P(x)\ \wedge\ Q(x))$为真（不用考虑 A 为假，因为 A 为假，那么 A->B 必然成立）

那么对于任意的值 v，P(v)和 Q(v)都成立。

由于对于所有的值 P(v)都成立，那么$\forall xP(x)$

类似地，由于对于所有的值 Q(v)都成立，那么$\forall xQ(x)$

因此可以推出$\forall xP(x)\ \wedge\ \forall xQ(x)$也成立

其次，B->A 的证明如下：

假设$\forall xP(x)\ \wedge\ \forall xQ(x)$为真

对于任意的 v，P(v)成立

类似的，对于任一的 v，Q（v）成立

所以，对于任意的 v，$P(v)\ \wedge\ Q(v)$成立

也就是对于所有的任意值 v，$\forall x(P(x)\ \wedge\ Q(x))$成立。

综上所述，该式$\forall x(P(x)\ \wedge\ Q(x)) \equiv \forall xP(x)\ \wedge\ \forall xQ(x)$成立

(11)用扩展欧几里得算法把 gcd(252, 356)表示成 252 和 356 的线性组合。(6 分)

根据要求用课件里的扩展欧几里得算法，得到 252*(-24)+356*17=4.

(12)求满足下列同余式的 x。(6 分)

Find all solutions, if any, to the system of congruences
$x \equiv 5 \pmod 6$, $x \equiv 3 \pmod{10}$, and $x \equiv 8 \pmod{15}$.

We cannot apply the Chinese remainder theorem directly, since the moduli are not pairwise relatively prime. However, we can, using the Chinese remainder theorem, translate these congruences into a set of congruences that together are equivalent to the given congruence. Since we want $x \equiv 5 \pmod 6$, we must have $x \equiv 5 \equiv 1 \pmod 2$ and $x \equiv 5 \equiv 2 \pmod 3$. Similarly, from the second congruence we must have $x \equiv 1 \pmod 2$ and $x \equiv 3 \pmod 5$; and from the third congruence we must have $x \equiv 2 \pmod 3$ and $x \equiv 3 \pmod 5$. Since these six statements are consistent, we see that our system is equivalent to the system $x \equiv 1 \pmod 2$, $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$. These can be solved using the Chinese remainder theorem (see Example 5) to yield $x \equiv 23 \pmod{30}$. Therefore the solutions are all integers of the form $23 + 30k$, where k is an integer.

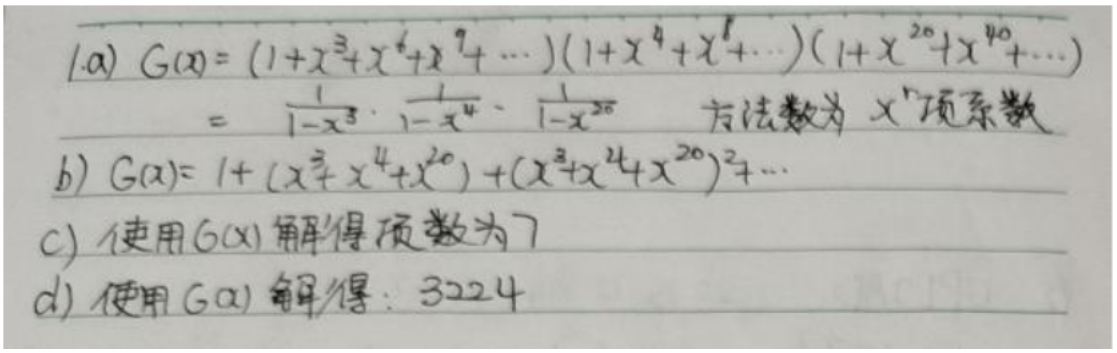
(13) 求解如何使用生成函数来计算使用 3 分、4 分和 20 分邮票将 r 分的邮资粘贴到信封上的方法数(分别考虑下述情况作答)。

a) 不考虑邮票顺序(无序)

b) 需要考虑邮票顺序(有序)

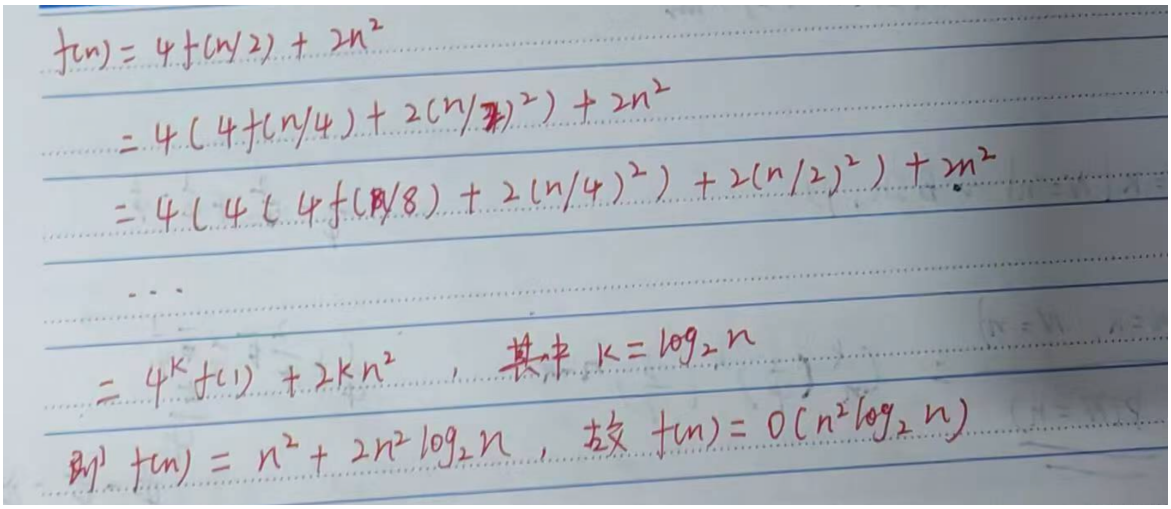
c) 根据 (a) 部分的答案，求解当邮票粘贴顺序无关时，使用 3 分、4 分和 20 分邮票将 46 分邮资粘贴到信封上的方法数。

d) 根据 (b) 部分的答案，求解当邮票粘贴顺序有关时，确定使用 3 分、4 分和 20 分邮票将 46 分的邮资按一排粘贴在信封上的方法数。(8 分)



(14) 设有某采用分而治之算法的时间复杂度可用递推式 $f(n)=4f(n/2)+2n^2$ 表示，且 $f(1)=1$，请给出 $f(n)$ 的渐进复杂度表示(大 0 表示)，要求写出具体求解过程。(6 分)

【答案 $O(n^2 \log n)$】



(15) a) 找到包含两个连续 0 或两个连续 1 的长度为 n 的三元字符串的数量的递

推关系。 三元字符串指仅包含 0、1、2 的字符串。

b) 初始条件是什么？

c) 有多少个长度为 6 的三元字符串包含两个连续的 0 或两个连续的 1？。(9 分)

解：a) 设 a_n 为长度为 n 且包含两个连续0或连续1的三元字符串数目

b_n 为既不包含两个连续0，也不包含连续1的三元字符串数目

对于 b_n，考虑以 2，1，0 结尾，对于 b_{n-1} 考虑以 0，1，2 结尾数

以2结尾：b_{n-1} 2 序号 - 即为 b_{n-1} ① b_{n-1} ② b_{n-1} ③

以1结尾：b_{n-1} ① 1 再合 b_{n-1} ③ 1 序号

以0结尾：b_{n-1} ② 0 序号 b_{n-1} ③ 0 序号

则 $b_n = 2b_{n-1} + b_{n-1}$ ③，又 b_{n-1} ② $= b_{n-2}$

则 $b_n = 2b_{n-1} + b_{n-2}$ 即 $(3^n - a_n) = 2(3^{n-1} - a_{n-1}) + 3^{n-2} - a_{n-2}$

则 $a_n = 2a_{n-1} + a_{n-2} + 2\cdot 3^{n-2}$

b) 则 $a_1 = 0$，$a_2 = 2$

c) 求 a_6，则由 b)，$a_3 = 10$ $a_4 = 40$ $a_5 = 144$

$a_6 = 2a_5 + a_4 + 2\cdot 3^4 = 490$

(16)构造 RSA 公钥密码体系的密钥，令 N=77， (9 分)

(a) 以 d = 13 为解密私钥，求对应的加密公钥 e；【-23】

(b) 求明文 25 对应的密文； 【53】

(c) 求密文 15 对应的明文。【64】

分 数	
评卷人	

三. 证明(每题 8 分，共 24 分)

(17)请用真值表方式证明下述推理是正确的；此外请验证是否可由(∀x)G(x)→(∀x)H(x)推导出(∀x)(G(x)→H(x))。[设 x 的个体域为{a,b}]。

(∀x)(G(x)→H(x))⇒(∀x)G(x)→(∀x)H(x)

(18) Show that if a and b are both positive integers, then $(2^a - 1) \bmod (2^b - 1) = 2^{a \bmod b} - 1$.

The statement we are asked to prove involves the result of dividing $2^a - 1$ by $2^b - 1$. Let us actually carry out that division algebraically—long division of these expressions. The leading term in the quotient is 2^{a-b} (as long as $a \geq b$), with a remainder at that point of $2^{a-b} - 1$. If now $a - b \geq b$ then the next step in the long division produces the next summand in the quotient, 2^{a-2b}, with a remainder at this stage of $2^{a-2b} - 1$. This process of long division continues until the remainder at some stage is less than the divisor, i.e., $2^{a-kb} - 1 < 2^b - 1$. But then the remainder is $2^{a-kb} - 1$, and clearly $a - kb$ is exactly $a \bmod b$. This completes the proof.

(19)用生成函数方法证明下述范德蒙德恒等式，其中 m, n, r 是非负整数，且 r<=m 或 n。

$$C(m+n, r) = \sum_{k=0}^{r} C(m, r-k)C(n, k),$$

由于 $(1+x)^n(1+x)^m = (1+x)^{n+m}$，对于等式左边有

$$(1+x)^n(1+x)^m = (\sum_{i=0}^{n} C_n^i x^i)(\sum_{i=0}^{m} C_m^i x^i) = \sum_{k=0}^{n+m} (\sum_{i=0}^{k} C_n^i C_m^{k-i}) x^k$$

而对于等式右边有

$$(1+x)^{n+m} = \sum_{k=0}^{n+m} C_{n+m}^k x^k$$

左右两边一比较可知

$$\sum_{i=0}^{k} C_n^i C_m^{k-i} = C_{n+m}^k$$

成立，证明完毕!