“离散数学（二）”样卷

解答内容不得超过装订线

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__假_或 0__.

(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__2__.

(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_36__种放法：

(4) 重新排列单词 MTAHEMATICS 中的字母能构成_4989600_或 4989599 个不同的串？

(5) 从 1、2、3、4……、11、12 这 12 个自然数中，至少任选__8__个，就可以保证其中一定包括两个数，它们的差是 7。

在这 12 个自然数中，差是 7 的自然树有以下 5 对：{12，5}{11，4}{10，3}{9，2}{8，1}。另外，还有 2 个不能配对的数是{6}{7}。可构造抽屉原理，共构造了 7 个抽屉。只要有两个数是取自同一个抽屉，那么它们的差就等于 7。这 7 个抽屉可以表示为{12，5}{11，4}{10，3}{9，2}{8，1}{6}{7}，显然从 7 个抽屉中取 8 个数，则一定可以使有两个数字来源于同一个抽屉，也即作差为 7.

(6) 27^{41} 除以 77 所得余数是___27___；

快速模指数直接求，或者费马小定理+中国剩余定理得 27。

(7) $(x+2y-4z)^6$ 展开式中 x^3y^2z 项的系数是__−960__。

多项式定理，可得$2^2(-4)^1\binom{6!}{3!\,2!\,1!}$=-960

二. 解答题

(8) 求命题公式(P→Q)∧(P→R)的主合取范式和主析取范式。（8 分）

解、$(P\rightarrow Q)\wedge(P\rightarrow R)$

$\Leftrightarrow(\neg P\vee Q)\wedge(\neg P\vee R)$ (合取范式)

$\Leftrightarrow(\neg P\vee Q\vee(R\wedge\neg R)\wedge(\neg P\vee(\neg Q\wedge Q)\vee R)$

$\Leftrightarrow(\neg P\vee Q\vee R)\wedge(\neg P\vee Q\vee\neg R)\wedge(\neg P\vee\neg Q\vee R)\wedge(\neg P\vee Q\vee R)$

$\Leftrightarrow(\neg P\vee Q\vee R)\wedge(\neg P\vee Q\vee\neg R)\wedge(\neg P\vee\neg Q\vee R)$(主合取范式)

$(P\rightarrow Q)\wedge(P\rightarrow R)$

$\Leftrightarrow(\neg P\vee Q)\wedge(\neg P\vee R)$

$\Leftrightarrow\neg P\vee(Q\wedge R)$(合取范式)

$\Leftrightarrow(\neg P\wedge(Q\vee\neg Q)\wedge(R\vee\neg R))\vee((\neg P\vee P)\wedge Q\wedge R)$

$\Leftrightarrow(\neg P\wedge Q\wedge R)\vee(\neg P\wedge\neg Q\wedge R)\vee(\neg P\wedge Q\wedge\neg R)\vee(\neg P\wedge\neg Q\ \neg R)$

$\vee(\neg P\wedge Q\wedge R)\vee(P\wedge Q\wedge R)$

$\Leftrightarrow(\neg P\wedge Q\wedge R)\vee(\neg P\wedge\neg Q\wedge R)\vee(\neg P\wedge Q\wedge\neg R)\vee(\neg P\wedge\neg Q\ \neg R)\vee(P\wedge Q\wedge R)$

(主析取范式)

其中主析取范式也可以写成

$$\equiv m_0 \vee m_1 \vee m_2 \vee m_3 \vee m_7$$

主合取范式也可以写成

$$\equiv M_4 \wedge M_5 \wedge M_6$$

(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：（6 分）

每个人有且仅有一个最好的朋友。

参考答案：

$\forall x\exists y\,(B(x,y)\ \wedge\forall z\,((z\neq y)\rightarrow\neg B(x,z)))$ 或者

$\forall x\exists y\forall z\,((B(x,y)\ \wedge(B(x,z)\rightarrow(y=z)))$

(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。(6 分)

$\forall x(P(x)\ \rightarrow\ Q(x))\ \Leftrightarrow\ \forall xP(x)\ \rightarrow\ \forall xQ(x)$

参考答案：个体阈为 D={a, b}, P(a)指定为：1，Q(b)指定为：0

P(a)指定为：0，Q(b)指定为：1，则$\forall x(P(x)\ \rightarrow\ Q(x))$为 0，

$\forall xP(x)\ \rightarrow\ \forall xQ(x)$为 1，故不等价。不成立

(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。（6 分）

解：作辗转相除：$1387=(-162)\times(-8)+91$，$-162=91\times(-2)+20$

$91=20\times4+11$，$20=11\times1+9$，$11=9\times1+2$，$9=2\times4+1$，$2=1\times2+0$

由此可得 $n=6$，$q_1=-8$，$q_2=-2$，$q_3=4$，$q_4=1$，$q_5=1$，$q_6=4$

$x=(-1)^{n-1}Q_n=73$，$y=(-1)^n p_n=625$，又 $(1387,162)=r_n=1$，

故 $1387\times73-162\times625=1=(1387,162)$

(12)求满足下列同余式的 x。(6 分)

$26x\equiv10 \pmod{62}$

参考答案： 三个数字同时除以 2，得到 $13x\equiv5 \pmod{31}$，据此得到 $x\equiv29 \pmod{31}$

(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。（8 分）

参考答案： $a_n=4a_{n-1}+5a_{n-2}$ (n>=3)

$a1=4,\ a2=21,\ a3=104,\ a4=521,\ a5=2604,\ a6=13021$

$a_n=(5/6)5^n+(1/6)(-1)^n$

(14)请用生成函数法，求方程 $x+y+z=14$ 满足 $1\le x\le8,\ 1\le y\le8,\ 1\le z\le8$ 的整数解的个数。(6 分)

参考答案：48

$(x^1+x^2+\ldots+x^8)(x^1+x^2+\ldots+x^8)(x^1+x^2+\ldots+x^8)=x^3(1+x+\cdots+x^8)^3$ 求展开式 x^{14} 的系数

(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？(6 分)

参考答案：使用容斥原理，其中 m=6，n=4。代入得 1560

(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 $N_B=77$, $e_B=13$。 (10 分)

(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]。

参考答案：

(a) 【17，-23】

$NA = 65 = 5 * 13$. 因此$(p-1)(q\ -1)$=48. 17 模$(p-1)(q\ -1)$的逆为d. 即

$d * 17 \equiv\ 1(mod\ \ 48)$, 可以$d$=17.

对于 Bob 而言

$NB = 77 = 7 * 11$. 因此$(p-1)(q\ -1)$=60. 13 模$(p-1)(q\ -1)$的逆为d. 即

$d * 13 \equiv\ 1(mod\ 60)$, 可以得$d$=-23. （d 为负数，应该还可以转换为 60 以下的正整数，所以 d=37）

(b) 先算 23^17 mod 65=43；再算 43^13 mod 77=43，得到答案 43

(c) 先算 43^(-23) mod 77=43 (或者 43^37 mod 77=43);再算 43^17 mod 65=23。

三. 证明

(17)证明若 $A \to (C \vee B), B \to \neg A$，则 $(D \to \neg C) \to (A \to \neg D)$ （8 分）。

p→q。可以 p 为真，然后证明 q 为真。

（1）¬A∨C∨B 前提

（2）¬ B ∨¬A 前提

（3）¬A∨C∨¬A 1 和 2 消解

（4）¬A∨C（由 3 得到）

（5）A→C (4 得到)

（6）D→¬C(附加前提)
（7）C→¬D (由 6 得到)
（8）A→¬D (由 5 和 7)
得证。

(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： $a^{pq} \equiv a \pmod{pq}$

证明：由 p，q 是两个不同的质数知（ p，q）=1。于是由 Fermat定理 $a^p \equiv a \pmod{p}$,

又由题设 $a^{q-1} \equiv 1 \pmod{p}$得到： $a^{pq} \equiv (a^q)^p \equiv a^p\,(a^{q-1})^p \equiv a^p \equiv a \pmod{p}$。

同理可证： $a^{pq} \equiv a \pmod{q}$。故： $a^{pq} \equiv a \pmod{pq}$。

(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（8 分）

$(1-x)^{-(n+1)}(1-x)^{-1} = (1-x)^{-n-2}$ （公式 1）

一方面：$\frac{1}{(1-x)^n}$=$\sum_{k=0}^{\infty} C(n+k-1,k)x^k$=$1+C(n,1)x+C(n+1,2)x^2+\cdots$

所以$\frac{1}{(1-x)^{n+1}}$=$\sum_{k=0}^{\infty} C(n+k,n)x^k$=$1+C(n+1,n)x+C(n+2,n)x^2+\cdots$

并且 $\frac{1}{(1-x)^{n+2}} = \sum_{k=0}^{\infty} C(n+k+1,n+1)x^k = 1+C(n+2,n+1)x+C(n+3,n+1)x^2+\cdots$

另一方面：$\frac{1}{1-x}$=$\sum_{k=0}^{\infty} x^k$=$1+x+x^2+\cdots$

因此公式 1 的右边可以表示为

$(1-x)^{-n-2} = \sum_{k=0}^{\infty} C(n+k+1,n+1)x^k$=$\sum_{m=0}^{\infty} C(n+m+1,n+1)x^m$

公式 1 的左边可以表示为

$$(1-x)^{-(n+1)}(1-x)^{-1}=\sum_{k=0}^{\infty} C(n+k,n)x^k * \sum_{k=0}^{\infty} x^k$$

$=\sum_{k=0}^{\infty}\sum_{j=0}^{k} C(n+j,n)\, x^k = \sum_{m=0}^{\infty}\sum_{k=0}^{m} C(n+k,n)\, x^m$