得分	评卷人

一. 单项选择（每小题 3 分，共 15 分）

(　　) 1.　10 种不同的球中选取 8 个，可重复选取，有几种取法

(A) C(18, 8)　　(B) C(18, 10)　　(C) C(17, 8)　　(D) C(17, 10)

这道题有部分同学记错了公式，选择了 D

(　　) 2.　n 个人围成一圈，有几种圈法

(A) n!　　(B) (n – 1)!　　(C) n^2　　(D) n^n

(　　) 3.　下面哪个递推式是常系数齐次线性递推式

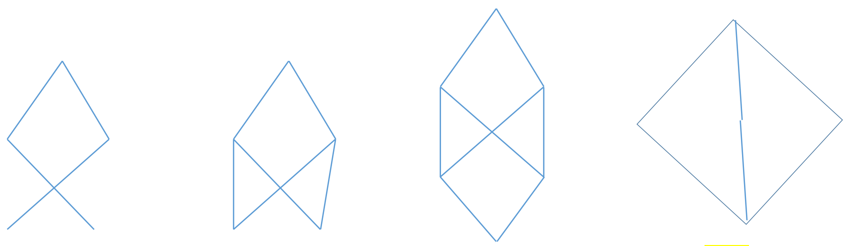
(A) $a_n = a_{n-1} + a_{n-2}$　　(B) $a_n = a_{n-1} + n$

(C) $a_n = n\, a_{n-1}$　　(D) $a_n = (a_{n-1})^2$

(　　) 4.　从 4 个花色 52 张扑克牌中，至少选出多少张牌才能保证至少有 3 张方块和 2 张梅花？

(A) 15 张　　(B) 14 张　　(C) 42 张　　(D) 44 张

（1） (　　) 5.　下列次序图(HASSE 图)哪个是格？



(A)　　(B)　　(C)　　(D)

得分	评卷人

二. 填空（每小题 3 分，共 15 分）

1. 3 个相同的白球和 3 个相同的黑球排成一排，有__20____种排法：

2. 集合 A、B，|A|=7，|B|=8，|A∪B|=12，则|A∩B|=__3____；

3. 集合 A 的基数是 5，B 的基数是 2，A 到 B 的满射有__30____个；

一些同学直接 2^5=32

4. (177*270）mod 31 = __19____；

这道题很简单，就算是直接把乘积算出来，再做一次除法，得到余数也都可以得出答案。

5. N 是正整数集，| 是其上的整除关系，在格(N; |)中，36 和 90 的最小上界是_180_____.

得分	评卷人

三. 解答题（50 分）

1. 有多少种排列方法，将 4 位男士和 3 位女士排成一排，使得一定有女士相邻？（6 分）

   解答：这道题很简单。前面课堂里学习过类似例题，如何将几位女生不相邻地排列于男生之间。

   那么总排列数 – 女生不能相邻的排列数 就是所要的答案。

   7 个人的总排列数是 P(7,7)

   女士不能相邻的数目：先将 4 为男生做排列，然后在四个男生的两边和中间插空选三个位置安排女生。 这个数是 P(4,4)P(5,3)

   所以题目答案是： P(7,7) – P(4,4)P(5,3) = 3600

   数字比赛很麻烦，只写表达式不写出最后答案的，还是要扣点分的。

出错情况 1：P(7,7) – P(4,4)C(5,3)

出错情况 2：有些同学是考虑如何先安排捆绑两格女生当成一个 P(3,2)，然后再求 P(6,6)。 得出结论：P(3,2)P(6,6)。 但是这里面有重复计数的。

2. 一个工厂逐月增长地定做体育赛车。如果在第 1 个月只做了 1 辆，在第 2 个月做了 2 辆，照此下去，第 n 个月做了 n 辆。对这个工厂的前 n 个月生产的赛车数构造一个递推关系。（6 分）

解答：假设用 a_n 表示前 n 个月生产的赛车数。那么：

$a_n = a_{n-1} + n$, for n $\geqslant$ 2, $a_1 = 1$

3. 4 个人（两男两女）分 10 块饼干，要求男的不能多余三块，女的不能少于两块。有多少种分法？（要求用生成函数）（6 分）

解：构造生成函数： $(1+x+x^2+x^3)^2(x^2+x^3+x^4+\ldots x^n+\ldots)^2$

$= x^4(1-x^4)^2/(1-x)^4= x^{12} /(1-x)^4 – x^4(2 x^4 - 1) /(1-x)^4$

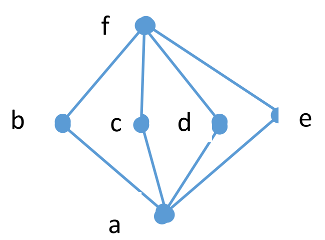
展开后 X^{10} 的系数即为所求， 答案是 64。

上面生成函数的展开式直接利用 $1/(1-x)^4$ 的展开公式就可以得出。

套用一下展开公式 $\frac{1}{(1-x)^n} = \sum_{k=0}^{\infty} C(n+k-1,k)x^k$

当然上面的生成函数的 $(x^2+x^3+x^4+\ldots x^n+\ldots)^2$ 可以改写为：$(x^2+x^3+x^4+\ldots+x^{10})^2$ 结果式一样的；改写成 $(x^2+x^3+x^4+\ldots+x^8)^2$ 也正确；

4. 下图对应的偏序集是一个分配格吗？为什么？（6 分）



5. 求解同余方程 $14x \equiv 9 \pmod{141}$. （6 分）

答案是 $x \equiv 51 \bmod 141$.

这道题利用辗转相除法， 求出 14 关于 模 141 的模逆， 就解出答案。

6. 假设 RSA 算法采用两个素数 7 与 13，选用 29 作为加密用的公钥。试求出解密的私钥 d; 并求出密文 4 对应的明文。（10 分）

解答：N=7Ｘ13=91, 91 的欧拉函数值是 72.

已知加密公钥 e=29, 利用 72 求出 29 关于模 72 的模逆 为 d=5, 这个模逆 5 就是 RSA 算法解密私钥;

密文 c=4, 明文 $M \equiv c^d \bmod(91) \equiv 4^5 \bmod 91 \equiv 23 \bmod 91$. 于是对应的明文是 23.

私钥 d=5, 明文是 23

7. 求解下面递推方程：$a_n = 7a_{n-1} - 10a_{n-2} + 4n + 3$, 其中 $a_0 = 7, a_1 = 14$.（10 分）

解答：这个递推方程式常系数线性非齐次的。 非齐次的函数部分是一个一次多项式函数 4n+3.

假设某组特解形如 $a_n = a \times n + b$. 将其带入递推关系得到

$a= -3 + 4$ 且 $b= -3b +16$, 由此求出 $a = 1, b = 4$. 于是得到递推方程的一个特解 $n + 4$.

相关齐次递推方程的特征方程为： $r^2 - 7r + 10 = 0$. 求得两个不同的特征根 $r1= 2, r2 = 5$, 于是相应的齐次递推方程的通解为：

$a_n = c1 \times 2^n + c2 \times 5^n$; 那么非齐次递推方程的解为： $a_n = c1 \times 2^n + c2 \times 5^n+n+ 4$

将初始条件带入到这个解中，求得系数 $c1 = 2, c2 =1$.

所以所以该方程的解是： $2^{n+1} + 5^n+ n+4$ for all $n\geq 0$

得分	评卷人

四.证明题（每小题 10 分，共 20 分）

1. 设 a, b, c 为正整数，a 整除 bc (即 a|bc), 且 gcd(a, b) = 1. 证明：a 整除 c.

这道题的得分率相对最低。 证明思路和方法也有多种。

证明思路方法 1：

因为 gcd(a, b) = 1， 也即 a, b 互素。 那么存在两个整数 s, t 使得 sa+tb = 1. 两边同乘以 c, 得到 sac + tbc = c. 由于 sac 显然能被 a 整除，bc 也是能被 a 整除的，所以两个能被 a 整除的数的和一定能被 a 整除。 于是 a|c 成立。证毕！

能用上 sa+tb = 1， 证明基本上就没问题了。

证明思路 2： 如果 a=1 或者 b=1 则显然结论成立。当 a>1,且 b>1 时，以下证明利用算术基本定律，任何一个正整数都可以唯一地分解为若干个素数的乘积。假设 a,b,c 三个整数的素数分解式如下：

$a = p_1^{i1}p_2^{i2}\dots p_s^{is}$

$b=q_1^{j1}q_2^{j2}\dots q_t^{jt}$

$c=r_1^{k1}r_2^{k2}\dots r_n^{kn}$

因为 gcd(a, b) = 1, a,b 互素，那么 a 的任何一个素因子 p_i 都不可能出现在 b 的素因子 $q_1q_2\dots q_t$ 之中。 否则，gcd(a, b) 就至少是 p_i 了。

$bc = q_1^{j1}q_2^{j2}\dots q_t^{jt} \times r_1^{k1}r_2^{k2}\dots r_n^{kn}$

由已知 a|bc, pi 就只能是在 $r_1^{k1}r_2^{k2}\dots r_n^{kn}$ 中出现了。并且 pi 的指数不会大于相应的某个素因子 r_k 的指数。由此得出 a|c.

证明思路 3：利用模逆存在. 由于 gcd(a, b) = 1, a,b 互素， 那么存在一个

b 的关于 mod a 的模逆 d，使得 $bd \equiv 1 \bmod a$.

因为已知 $a|bc$，所以 $bc \equiv 0 \bmod a$. 两边乘以模逆 d，得到 $c \equiv 0 \bmod a$.

于是得到 $a|c$.

当然这个地方有少部分同学不是用模逆乘两边，而是两边同除以 b. 这样有点理由不足。除非说清楚用到的一个性质或者定理。因为作为同余式，两边不能同除的。只有用到一个定理。需要把这个定理或者性质说明一下，相当于同乘以模逆。

证明思路 4：因为 $\gcd(a, b) = 1$，所以 $\mathrm{lcm}(a,b) = ab/\gcd(a,b) = ab$.
$a|bc$, $b|bc$，所以 $\mathrm{lcm}(a,b)|bc$. 于是有 $ab|bc$，这样也就能推出 $a|c$.
当然，这里的证明一句话都不能少。否则理由不充分或者是叙述不清。

2. x, y, z 是格 L 中的元素，证明：$(x \wedge y) \vee (x \wedge z) \leq x \wedge (y \vee z)$.
这道题的证明是基础的，没有多少别的方法，所用到的也就是可传递性，上界、下界、最大下界和最小上界的基本概念的理解。