1. 黑白红三种球各三个的排列数　是 1680. 这道题实际上是有重复排列, 同一种颜色的球是不可识别的，不加区分的。所以这个排列也就是 C(9,3)C(6,3)=1680. 这是基础题，课堂上讲过例题，同学们也做过类似的作业。 还是有不少同学没有得到这各分数。
2. 从大量黑红白的球中，组合成 10 个，这是典型的有重复组合问题。直接套公式即可。C(10+3 -1, 3-1) = 66.　也可以列出模型 x+y+z=10,　求整数解的个数。
3. 钞票组合问题：现有 1 元的钞票 5 张，10 元钞票 4 张，50 元钞票 3 张，试问：

   能组合出多少种额度的钞票组合?

这道题目的答案是 119 中组合（不包括 0 元的）；包括零元的就是 120 种。题目并没有写清楚是否包含 0，所以，这次阅卷无论是 119 还是 120 都给满分。

其实这道题就是利用乘法原理，一道简单的计数题目。

这道题的做法有两种:

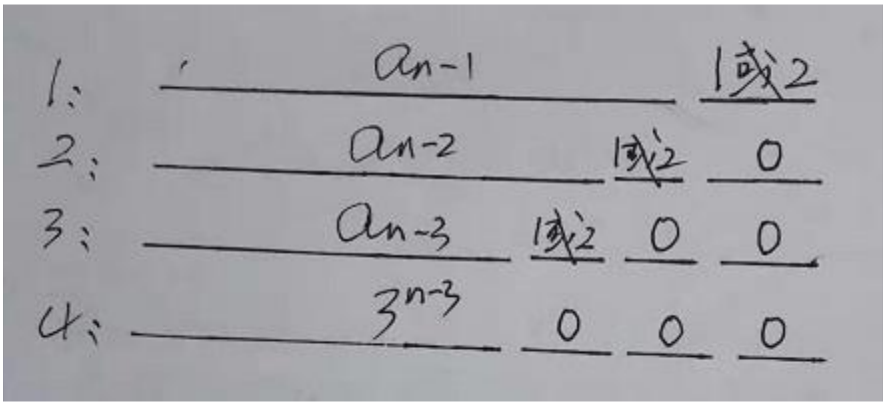
(1) 由于三种面值的钞票的数量的特殊性，在组合成额度时不会相互影响，所以计算能形成多少种额度时，就是简单的 $6*5*4-1=119$；　包括一张都不选的话就是 $6*5*4=120$

当然如果这道题目的备用钞票数如果不是这样特殊，比如将 1 元钞票的备用数量改成 10 张，问题就复杂多了。

（2）第 2 类做法就是构造一个正确的生成函数 G(x), 该函数由 3 个部分的乘积组成。对于这个生成函数，根据题目要求，需要统计的不是每一个 x^k 项的系数，而是要计数有多少个不同的 x^k 项。 只要是生成函数写出来了，即使没有展开计算初结果，就已经至少一半的分数了，当然需要说明在这个生成函数下，哪个数是题目要求的结果。这道题用生成函数的，最后计算结果正确的不多。

考试要求里面有说钱币组合，而且这个组合还是比较简单的数字。

4. 此次考试，得分率最低的是“有 3 个连续 0 的三进制数的递推关系模型”问题。老师们



没有想到这道题得分率如此之低。 三进制于二进制方法上没有什么区别，只是数量上有区别。同学们做过两个连续 0 的二进制的递推关系的题目，3 个连续 0 就复杂些

解：假设 n 位长的有 3 个连续 0 的三进制数的个数为 a_n，对于个一 n 位长的三进制数，先分析最后一位是 0 还是非 0，参考下面的图，有四种情况：

Case 1： 这种情况下，个数是 $a_{n-1}*2$

Case 2: 这种情况下， 个数是 $a_{n-2}*2$

Case 3: 这种情况下， 个数是 $a_{n-3}*2$

Case 4： 这种情况下，后面已经有 3 个连续 0 了，前面的 n-3 位长的三进制数，无论怎么都满足条件，个数位 3^{n-3};

因此 这个递推关系为： $a_n = 3^{n-3} + 2a_{n-1} + 2a_{n-2} + 2a_{n-3}$

有些同学没有看清楚题目，当二进制处理；更多的是不知道从哪里下手。

初始条件是： a0=0,a1=0, a2=0, a3=1.

部分同学写出了几个初始条件，但递推关系没能写出来。 也有的同学写出了递推关系，却没有写初始条件。

5 求解递推方程： 得分率还行，但比预期低。，部分不知道怎么做的同学只能写出特征方程和特征根。有同学特征根求解错误；也有同学求出了特征根，没有写出通解；

这是一个典型的 2 阶常系数线性非齐次递推方程；特征方程和特征根都容易求出来；

但是一些同学在求特解时陷入了一次多项式的陷井。这里的多项式是一个二次的，没有想到用二次试一试，就很难解下去。

解：特征方程为 $r^2 - 3r + 2 = 0$， 特征根分别是 1 和 2. 所以通解形式为：

$a_n = k_1*1^n + k_2*2^n$； 特解为 2 次的多项式： $a_n = -n^2-4n$

最后的解为： $a_n = 2^{n+2} - n^2-4n - 4$

6. 求方程 $x + y + z = 12$ 满足 $1\le x, y, z \le 5$ 的正整数解的个数。

这道题是利用生成函数求解带限定条件的不定方程的标准题型。

出现的问题: 一是有些同学不知道构造生成函数; 更多的是对条件"$1\le x, y, z \le 5$"理解错误。有同学理解 x 大于等于 1, y 没有限制, z 小于等于 5. 在这种错误的理解下, 构造的生成函数就完全不一样了, 当然最后结果必然错误 (不过, 这次阅卷对于这种错误理解条件的, 还是给了不少分)。这种类型的条件表达方式是常见的。 答案很简单就是 10.

7. 5 个不同的球放入 3 个不可区分的盒子, 且每个盒子都非空, 有__25____种放法。

8. "八仙过海"的题目: 这其实就是 8 个元素对 3 个元素的满射的数量的问题。上课时讲过的第一个例题就是 6 个元素对 3 个元素的满射的数量的求法, 进一步推出了 M 个元素对 N 个元素的满射的数量的求解方法。公式不用背, 但求解方法一模一样, 就是容斥原理的使用。 有些同学不会做, 更有部分同学 (还不少), 就是硬拼凑, 把所有可能出现的情况凑出来。如果凑完整正确了也给满分, 但这种做法近乎"暴力"解法。

这道题目主要考大家理论联系实际, 能把实际问题转换为数学问题的能力。

一部分同学就是简单地写出了计算的数字表达式 $3^8 - 3*2^8 + 3 = 5796$, 没有任何过程, 没有任何说明, 这是要扣分的, 不是填空题。 也有同学写出了计算的过程和求满射的表达式, 但是对于表达式里面的符号所代表的含义没有任何说明, 也是需要扣分的。

这个题的得分率也不是很高。

有同学写出表达式 $A(8,3)*3^5$, 这个意思是先选 3 个人分别对应 3 种过河方式。但这个表达式里面存在着大量的重复计数, 是错误的。

9. 1—20 中最多能取___9___个数, 使得其中任何两数都是互素的

这道题正确率不高。{1,2,3,5,7,11,13,17,19}, 也可以是 {1,2,9,5,7,11,13,17,19}

10. $23^{1002} \equiv$ __37____ (mod 41). 41 是一个素数, 23 与 41 互素, 直接利用费尔马小定理, 就能得到 $23^{1002} \equiv 23^2 \bmod (41)$, 很快就能算出余数是 37.

11. 求最大公约数是基础题

12. 求解同余式 $2^{10}x \equiv 5 \pmod{123}$。 $2^{10} \bmod 123 = 40$，所以该同余方程等价于

$40x \equiv 5 \pmod{123}$. 40 与 123 是互素的，只要求出相关的模逆，就解出来，刚好模逆也是 40. 解为 $x \equiv 77 \bmod (123)$，也可以表达为 $x = 77 + 123k$，其中 k 为整数。

这道题为求解同余方程式的基础题，不需要特别技巧，没有难度。

有同学只写了一个解 77，是不对的，会扣分；也有同学什么过程都没有，直接写了一个 77 作为答案。

13. RSA 计算题：

(1) 少部分同学欧拉函数值计算错误；已知私钥不知道如何求公钥。私钥与公钥是关于欧拉函数值这个模数互为模逆的。

(2) 公钥计算过程错误或以负数作为公钥导致密文计算错误

(3) 明文密文加解密算法混淆了私钥、公钥
本来是用公钥对明文进行加密，来求解密文；用私钥解密对密文进行解密，得到明文。但是不少同学搞反了，用私钥加密 $6^{17} \bmod (55)$，公钥解密 $4^{33} \bmod (55)$。

(4) 明文密文加解密时，模数采用的是欧拉函数的值而不是两个大素数的乘积
不少同学犯的错误，不是用两个素数的乘积作为模数来求密文和明文，而是用欧拉函数值作为模数。 RSA 加解密的算法中，欧拉函数值是保密的。

(5) 明文密文求解计算错误

(6) 少数人完全不知道如何入手

很多人只拿到了一求公钥的这个分数，后面全搞错，很遗憾。 这道题是没有难度没有技巧的，也就是基本要求。

正确的应该是：

$\Phi(5*11) = 40$，已知解密私钥 d = 17，所以加密公钥 $e*d \equiv 1 \bmod (40)$，解出加密公钥为：$e = 33$;

密文 4 解密后对应的明文应该是 $4^{17} \bmod (55) = 49$;

明文 6 加密后对应的密文应该是 $6^{33} \bmod (55) = 51$

14. 数论的证明题，方法五花八门，正确的不少于 5 种。

同学们做过一道 $42 \mid (n^7 - n)$ 的证明题，基本上差不多。 不会做的很遗憾。

下面是 3 种证明方法:
证法 1: 整数 18 的欧拉函数值与整数 9 的欧拉函数值是一样的, 都等于 6;
由于 n 跟 6 互素, 18 的素数因子也是 2, 3, 所以 n 与 18 也互素。直接利用欧拉定理, 有 n^6 mod 18 余 1, 于是 n^6 -1 能被 18 整除, 故 18 整除 n^7 -n

证法 2: 整数 9 的欧拉函数值是一样的, 都等于 6;
由于 n 跟 6 互素。直接利用欧拉定理, 有 n^6 mod 9 余 1, 于是 n^6 -1 能 9 整除; 再者, 因 n 与 6 互素, 所以 n 必然是奇数; 于是 n^6 -1 必然是偶数, 能被 2 整除。2 与 9 是互素的, 分别都整除 n^6 -1, 所以 18 也必然整除 n^6 -1。 故 18 整除 n^7 -n

证法 3:
由于 n 跟 6 互素, 所以 n mod 6 余 1 或者是 5, 不可能余 0, 2, 3, 4; 于是 n= 6k+1 或者 n = 6k -1. 再分析 $(6k-1)^6 - 1$ 或者 $(6k+1)^6 - 1$ 都能被 18 整除即可。

实际上, 这个数都可以被 36 整除, 当然证明起来稍微麻烦些;

出现的主要问题是:
很多人不会用欧拉定理, 在使用欧拉函数值的时候, 简单认为 6 的欧拉函数值为 5 (6 不是素数, 所以错误), 或者说 18 的欧拉函数值用 17.
有些同学完全没有办法动笔

15. 组合分析法证明题:
一般的方法:
也有用类似于生成函数展开, 二项式展开的系数来分析证明的, 也可以。

证明中出现的问题
(1) 用代数方法证明, 直接用组合公式代入证明两边相等, 不给分。
(2) 用范德蒙恒等式证明, 严格来说也不符合要求。除非对该恒等式进行组合意义解释
(3) 把问题对应于 2n 个物品、2n 个球、2n 个数、2n 个项等, 很多人都没有说明是不同的物品、不同的数、不同的项;
(4) 将 2n 个人或物分成两堆或者两组, 分别取组合数的方法没有问题。但有少部分人, 并没有说明这两组都应该是 n 个! 这是要扣分的。
(5) 大部分同学都是用 2n 个元素的集合, 分成两个 n 个元素的子集。 但严格来说这里应该是两个不相交的、元素个数分别是 n 的子集。
(6) 也有部分同学, 是先有两个集合 A、B, 各有 n 各元素, 然后将 A 与 B 并起来, 在这个情况下来证明。思路没问题。但是也有问题, 是没有说明 A 与 B 不相交。如果 A 与 B 有共同元素, 就有问题了。数学证明要求是严谨严格的。
(7) 有些同学完全没有证明出来。