1. (a)

x	p(x)	q(x)	r(x)
0	3	1	0
1	1	0	2
2	3	3	0
3	1	2	2

p, q intersect

(b)

x	p(x)	q(x)	r(x)
0	3	2	0
1	0	1	3
2	2	0	1
3	4	4	4
4	1	3	2

p, q, r intesect

(c)

(c)

x	$p(x)$	$q(x)$	$r(x)$	
0	3	3	0	p, q intersect
1	5	2	4	
2	1	1	2	p, q intersect
3	3	0	0	
4	5	5	4	p, q intersect
5	1	4	2	

(d) in R, $p(x) = q(x) \Rightarrow 3x + 6 = 0$, $x = -2$, as well as Q

$p(x) = r(x) \Rightarrow 4x + 3 = 0$, $x = -\frac{3}{4}$, as well as Q

~~R,~~ part (b), because mod 5 has an inverse for $\frac{1}{4}$, which is 4, so $x = -3 \cdot (4) = -12$

$= 3 \mod (5)$, which gives an intersection on (b).

(e) (i) $x \equiv 2, y \equiv 2 \mod 4$ counterexample, false.

(ii) True, because WLOG $x \not\equiv 0 \pmod 5$, then

, which gives an intersection on (b).

(e) (i) $x \equiv 2, y \equiv 2 \mod 4$ counterexample, false.

(ii) True, because WLOG $x \not\equiv 0 \pmod 5$, then there exists an inverse x^{-1}, so $(x^{-1})(xy) \equiv (x^{-1})0 \mod 5$,

or $y \equiv 0 \mod (5)$.

(iii) $x \equiv 2, y \equiv 3 \mod (6)$ counterexample.

Case mod 5 is most similar because 5 is a prime, hence there exist an inverse for every number, which maps to "division".

2. (a) $p(x) = \dfrac{(x-1)(x-2)}{(0-1)(0-2)} \cdot 1 + \dfrac{(x-0)(x-2)}{(1-0)(1-2)} \cdot 1 + \dfrac{(x-0)(x-1)}{(2-0)(2-1)} \cdot$

$= x^2 - x + 1$

(b) Taking finite differences of $x=1$ jumps, we have $\Delta((-1,3),(0,1),(1,1),(2,3))$

$= (2, 0, -2)$, which is linear which means polynomial exists. It is: $x^2 - x + 1$.

(c) $x^2 - x + 1$ is the unique polynomial (and only) through the first 3 points, but $(-1,0)$ does not fit into the

It is: x^2-x+1.

(c) x^2-x+1 is the unique polynomial (and only) through the first 3 points, but $(-1,0)$ does not fit into this polynomial, so no.

(d) Apply Lagrange interpolation on the first 3 points to get a polynomial P of degree 2 or lower. Now check if the 4-th point satisfies P, return the result.

(e) Apply the algorithm in (d) to all 5 cases, return the index of the excluded point when the algorithm returns true for the other 4 points.

it is: x^2-x+1.

(c) x^2-x+1 is the unique polynomial (and only) through the fist 3 points, but $(-1,0)$ does not fit into this polynomial, so no.

(d) Apply Lagrange interpolation on the fist 3 points to get a polynomial P of degree 2 or lower. Now check if the 4-th point satisfies P, return the result.

(e) Apply the algorithm in (d) to all 5 cases, return the index of the excluded point when the algorithm returns true for the other 4 points.

3. (a) We have that:

(1) $c \equiv 1 \pmod 2$

(2) $c \equiv 2 \pmod 3$

(3) $c \equiv 1 \pmod 5$

(4) $c \equiv 3 \pmod 7$

(5) $c \equiv 1 \pmod{11}$

(1) and (2) imply $c \equiv 5 \pmod 6$, and (3) implies

$c \equiv 11 \pmod{30}$, (4) implies $c \equiv 101 \pmod{210}$,

and (5) implies $\underline{c \equiv 2201}$ $\pmod{2310}$, the code.

(b) We pick a random polynomial of de

), the code

(b) We pick a random polynomial of degree 2 in some finite field ~~so that~~ such that $p(0) = c$. Give $p(1), \ldots, p(5)$ to the elders respectively. If 3 points are known, p is formed uniquely, while having only 2 points cannot, so we are done.

(c) He knows it's of the form

$$p(x) = q \cdot (x - x_1)(x - x_2) + \frac{(x - x_2)}{(x_1 - x_2)} y_1 + \frac{(x - x_1)}{(x_2 - x_1)} y_2$$

where q is some constant, since

$p(x_1) = y_1$, $p(x_2) = y_2$, our given points, but that is all.

4. (a) We send 27 packets. Thus at most 9 packets get erased, but we will still have 18 packets, or 18 coordinates to reconstruct the original polynomial of degree 17 that encoded the 18 packets, (with encoding $P(1) = c_1$, $P(2) = c_2 \ldots$ $P(18) = c_{18}$).

(b) Using the general error method written in the handout, we need

... if we are sending a

(b) Using the general error method written in the handout, we need $n+2k$ packets if we are sending a n-length message and k is the corruption. But from the question, $k \le \frac{n}{5}$, and $n=18$, so we should transmit at least $18 + 2 \cdot \frac{18}{5}$ packets, or at least 26 packets.

5 (a) $\binom{52}{13}$

(b) 48 cards w/ no aces, so $\binom{48}{13}$

(c) Pick 4 cards aces so 48 left, need to pick 9, so $\binom{48}{9}$. [illegible]

(d) 13 spades choose 5, then choose remaining 8 from $52-13=39$, so $\binom{13}{5}\cdot\binom{39}{8}$.

(e) Every card has its counterpart in the other deck, so there are 2^{52}

from $52-13=39$, so $\binom{13}{5} \cdot \binom{39}{8}$.

(e) Every card has its counterpart in the other deck, so there are 2^{52} swaps per position that's unique so if we considered every one of 104 unique, we have

$$\frac{(104!)}{(2^{52})}.$$

(f) $\binom{17}{6}$, choose 6 spots out of 17.

(g) $\dfrac{\underline{\text{total} - \text{strings w/ equal number of 1 and 0}}}{2} = \dfrac{2^{66} - \binom{66}{33}}{2}$,

by symmetry, since # strings w/ more 1's = # strings w/ more 0's.

(h) K appears twice, 8 letters total, so

$$\frac{8!}{2!}$$

(i) 3 A's, so $\frac{6!}{3!}$

(j) 2 I's, 2 A's, so $\frac{10!}{2! \cdot 2!}$

(k) 4 S's, 4 I's, 2 P's, so $\frac{11!}{4!4!2!}$

(k) 4 S's, 4 I's, 2 P's, so $\frac{11!}{4!4!2!}$

(l) ~~stars and bars~~ Each ball has one of 24 bins to go to, so 24^8.

(m) Using stars and bars (or bins), we have $\binom{8+23}{23} = \binom{31}{23}$

(n) Assign each bin a ball, so 3 balls are left, however we assign them. This is a stars and bars problem, so we have $\binom{7}{4}$.

(o) Arrange 30 in a line, and pick the person to be paired with the first person in line. 29 ways to do this, then remove the pair. Then there are 27, … 25, …

So, $29 \cdot 27 \cdot 25 \ldots \cdot 3 \cdot 1$.

6. (a) For $k = 0, 1, \ldots, n$,

pick k males and $n-k$ females, which is

$\binom{n}{k}\binom{n}{n-k} = \binom{n}{k}^2$ ways. Summing these up

is the same as choosing n people among the total

$2n$ people, so

$$\binom{2n}{n} = \sum \binom{n}{k}^2.$$

(b) It's not possible to assign fellowships when we're choosing 0 boys or 0 girls, so

$k = 1, 2, \ldots, n-1$ are only valid. Each time

$\binom{\ }{n} = \sum \binom{\ }{k}^2.$

(b) It's not possible to assign fellowships when we're choosing 0 boys or 0 girls, so

$k = 1, 2, \ldots, n-1$ are only valid. Each time we pick k males, $n-k$ females for seats, we have $k \cdot (n-k)$ ways to assign each group a fellowship,

so total $= \displaystyle\sum_{k=1}^{n-1} k(n-k)\binom{n}{k}\binom{n}{n-k}.$

But this is the same as first giving the fellowships to a boy and a girl, which is n^2 ways, then taking the leftover $n-2$ from $2n-2$, so

$n^2 \cdot \binom{2n-2}{n-2}.$

(c) You have n candidates and you may pick any number ≥ 1 as a vicepresident, then promote one of the VP's to a president.
This is the sum

$$\binom{n}{1} + 2 \cdot \binom{n}{2} + \dots + n\binom{n}{n}$$ by picking

the VP's first then assigning presidency.
This is also the same as choosing the president first, then forming the group of VP's from remaining,
so $n \cdot 2^{n-1}$!