1)

You are given a black box f which contains either: (World 1) 3 coins, and with each invocation the 3 coins are all flipped and the number of heads is returned; or (World 2) a 4-sided die, numbered 0-3, and with each invocation the die is rolled and the resulting number is returned.

What is the advantage of the following distinguisher? Answer as a reduced fraction with no spaces, or 0 or 1 if appropriate.

```
result = f()
if (result == 0)
   output "4-sided die"
else
   output "3 coins"
```

$$\text{Advantage} = \Pr[\text{output dice} \mid f \text{ is dice}] - \Pr[\text{output dice} \mid f \text{ is coins}]$$

$$= \frac{1}{4} - \frac{1}{2^3}$$

$$\boxed{\text{Advantage} = \frac{1}{8}}$$

2)

The distinguishing algorithm in the previous Question is not optimal. What is the maximum achievable advantage when the distinguisher is allowed to invoke f only once.

Answer as a reduced fraction with no spaces, or 0 or 1 if appropriate.

Advantage = Pr[output dice | f is dice] - Pr[output dice | f is coins]

result	3 coin	4 sided
0	$\frac{1}{8}$	$\frac{1}{4}$
1	$\frac{3}{8}$	$\frac{1}{4}$
2	$\frac{3}{8}$	$\frac{1}{4}$
3	$\frac{1}{8}$	$\frac{1}{4}$

$\frac{1}{8} < \frac{1}{4}$

$\frac{3}{8} > \frac{1}{4}$

Since 0 or 3 is more likely to occur, we will change the algorith to the following

```
result = f()

if result == 0 or result == 3

    output "4-sided dice"

else
    output "3 coins"
```

3 ways to get 1 head:

C1	C2	C3
1	0	0
0	1	0
0	0	1

Let: 1 be head
0 be tail

3 ways to get 2 heads:

C1	C2	C3
1	1	0
1	0	1
0	1	1

$$\frac{\text{\# of conditions in if statement}}{\text{\# of total outcomes}}$$

$$\text{Advantage} = \frac{2}{4} - \left(\frac{1}{8} + \frac{1}{8}\right)$$

$$= \frac{1}{2} - \frac{1}{4}$$

$$\boxed{\text{Advantage} = \frac{1}{4}}$$

3)

If f: $Z_{10} \rightarrow Z_{10}$ is a random permutation, what is the probability that any pair of f(0), f(1), or f(2) are equal? Answer as a reduced fraction with no spaces, or 0 or 1 if appropriate.

0 because a permutation doesn't allow duplicate values

4)

If f: $Z_{10} \rightarrow Z_{10}$ is a random function, what is the probability that any pair of f(0), f(1), or f(2) are equal? Answer as a reduced fraction with no spaces, or 0 or 1 if appropriate.

Hint: The probability that any of the pairs match is 1 minus the probability that none of them match. To calculate the probability that none of them match, imagine filling in the definition of f as a table, one entry at a time. What is the probability f(1) mismatches f(0)? What is the probability that f(2) mismatches both f(0) and f(1), given that f(1) mismatches f(0)? What is the probability that both these events occur? (It's the product)

Advantage = Pr[output func | any of f(0), f(1), or f(2) are same)

- Pr[output func | none match]

$= 1 - \left[\frac{9}{10} \times \frac{8}{10} \right]$

$= \boxed{\frac{7}{25}}$

$\frac{9}{10}$ is the probability 0 doesn't equal 1

$\frac{8}{10}$ is the probability 2 doesn't equal 0 and 1, given that 0 and 1 are not equal

5) You are given a black box f which contains either:
(World 1) f: $Z_{10} \to Z_{10}$ which is a random function; or
(World 2) f: $Z_{10} \to Z_{10}$ which is a random permutation.

What is the advantage of the following distinguisher? Answer as a reduced fraction with no spaces, or 0 or 1 if appropriate.

```
if (any of f(0), f(1) or f(2) are the same)
   output "random function"
else
   output "random permutation"
```

Advantage = Pr[output func | any f are same]

− Pr[output func | none f are same]

$$= \frac{7}{25} - 0 \qquad \text{Problem 4} - \text{Problem 3}$$

$$\boxed{\text{Advantage} = \frac{7}{25}}$$