Let $f : \mathbb{Z}_{10} \rightarrow \mathbb{Z}_{10}$ be a random function. What is the probability that $f(0) = 0$ and $f(1) = 1$? Express your answer as a reduced fraction without any spaces (eg, 1/3 and not 12/36), or as 0 or 1 if appropriate.

$$p(A \text{ and } B) = p(A) * p(B)$$

$$= \frac{1}{10} * \frac{1}{10}$$

$$= \frac{1}{100}$$

Let $f : \mathbb{Z}_{10} \rightarrow \mathbb{Z}_{10}$ be a random permutation. What is the probability that $f(0) = 0$ and $f(1) = 1$? Express your answer as a reduced fraction without any spaces (eg, 1/3 and not 12/36), or as 0 or 1 if appropriate.

$$p(A \text{ and } B) = p(A) * p(B|A)$$

$$= \frac{1}{10} * \frac{1}{9}$$

$$= \frac{1}{90}$$

You are given a black box $f : \mathbb{Z}_{10} \rightarrow \mathbb{Z}_{10}$ that contains either a random permutation or a random function. Your distinguisher is allowed to invoke f twice. What is the best advantage you can achieve? Express your answer as a reduced fraction without any spaces (eg, 1/3 and not 12/36), or as 0 or 1 if appropriate.

$$\text{Advantage} = \Pr[\text{right}] - \Pr[\text{wrong}]$$

$$= \Pr[\text{output func} \mid f \text{ is func}]$$

$$- \Pr[\text{output func} \mid f \text{ is perm}]$$

$$= \frac{1}{10} - 0$$

$$= \frac{1}{10}$$

You are given a black box f() that contains either a fair coin or a pair of six-sided dice. If f() is a pair of dice, then each invocation of f() rolls the dice, sums the die faces, and reports 0 if the sum is even and 1 if the sum is odd. If f() is a coin, then each invocation of f() flips the coin and reports 0 if it's heads and 1 if it's tails. What is the advantage of the following distinguisher?

```
if f() == 0
   output "dice"
else
   output "coin"
```

The intuition behind this distinguisher is that there are 6 possible even dice outcomes and only five odd ones. Enter your answer as a reduced fraction without any spaces (eg, 1/3 and not 12/36), or as 0 or 1 if appropriate. Note that the probability that a pair of dice sum to 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12 is 1/36, 2/36, 3/36, 4/36, 5/36, 6/36, 5/36, 4/36, 3/36, 2/36, 1/36.

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

pair dice

Even sum : 2, 4, 6, 8, 10, 12

1/36, 3/36, 5/36, 5/36, 3/36, 1/36

$$\left(\frac{1}{36} + \frac{3}{36} + \frac{5}{36} + \frac{5}{36} + \frac{3}{36} + \frac{1}{36}\right) - \frac{1}{2}$$

Advantage = 0

5 2 / 2 points

Let's say the following code is executed on a little-endian computer.

```
uint32_t *p = malloc(8);
p[0] = 0x12345678;
p[1] = 0x23456789;
```

What are the 8 bytes in memory that begin at the address that's in p? Express as 8 two-digit hexadecimal values with a single space between each (eg, ab cd ef 01 02 03 04 50).

1) Starting at p[0], read each byte in Little Endian

78 56 34 12

2) Now from p[1], read each byte in Little Endian

89 67 45 23

3) Write all bytes starting from p[0] results

78 56 34 12 89 67 45 23