EOM Quiz 1

Due Sep 23 at 10pm	**Points** 20	**Questions** 6	
Available Sep 23 at 9am - Sep 23 at 10pm		about 13 hours	**Time Limit** 40 Minutes

Instructions

This is your end-of-module quiz. There is also a separately timed part on Mimir. Unlike the old quiz you did for homework, it is not collaborative. Once you start the quiz you will have a limited amount of time to complete it.

Be careful with formatting. If I specify a formatting method and you do not follow it, you will lose some credit.

The quiz is open notes. You may use your own notes and any of the resources on the course webpages. You are not allowed to use the internet for any other purpose unless a question directs you to do so.

On the day of the quiz, do not use any public forum to ask any quiz-related questions. Once you see the quiz, do not discuss it with anyone until the quiz closes for everyone.

Good luck!

This quiz was locked Sep 23 at 10pm.

Attempt History

	Attempt	Time	Score
LATEST	Attempt 1	40 minutes	7 out of 20

ⓘ Correct answers are hidden.

Score for this quiz: **7** out of 20
Submitted Sep 23 at 4:17pm
This attempt took 40 minutes.

Question 1	**2 / 2 pts**

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"
```

1/8

Inanswered

Question 2

0 / 2 pts

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.

Incorrect

Question 3

0 / 2 pts

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.

1/10

Incorrect

Question 4

0 / 2 pts

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)

9/5

Incorrect

Question 5

0 / 2 pts

You are given a black box f which contains either: (World 1) f: $Z_{10} \rightarrow Z_{10}$ which is a random function; or (World 2) f: $Z_{10} \rightarrow Z_{10}$ 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"
```

1

Unanswered

Question 6

5 / 10 pts

This question is a placeholder for your Mimir score. You can ignore it.

The Mimir part is separately timed.

Your Answer:

Quiz Score: **7** out of 20