

HW 06 CMSC/MATH/ENEE 456. Morally DUE Oct 26

1. (0 points) What is the day and time of the timed part of the midterm?

GOTO NEXT PAGE

2. (40 points) In this problem you will use the ideas behind Pollard's ρ -algorithm to factor 143, 371, and 551.

(a) (15 points) Let $f(x) = x^2 + 1 \pmod{143}$. Let $x_0 = 7$.

Compute

$x_1 = f(x_0)$, $x_2 = f(f(x_0))$, $\dots$ until you have two numbers x_i and x_j whose difference $|x_i - x_j|$ is NOT relatively prime to 143.

Write down:

i is $\dots$

j is $\dots$

x_i is $\dots$

x_j is $\dots$

$GCD(|x_i - x_j|, 143)$ is $\dots$

(The GCD should be a factor of 143).

GOTO NEXT PAGE

- (b) (10 points) Let $f(x) = x^2 + 1 \pmod{371}$. Let $x_0 = 7$. Compute $x_1 = f(x_0)$, $x_2 = f(f(x_0))$, $\dots$ until you have two numbers x_i and x_j whose difference $|x_i - x_j|$ is NOT relatively prime to 371.

Write down:

i is $\dots$

j is $\dots$

x_i is $\dots$

x_j is $\dots$

$GCD(|x_i - x_j|, 371)$ is $\dots$

(The GCD should be a factor of 371).

GOTO NEXT PAGE

- (c) (15 points) Let $f(x) = x^2 + 1 \pmod{551}$. Let $x_0 = 7$. Compute $x_1 = f(x_0)$, $x_2 = f(f(x_0))$, $\dots$ until you have two numbers x_i and x_j whose difference $|x_i - x_j|$ is NOT relatively prime to 551.

Write down:

i is $\dots$

j is $\dots$

x_i is $\dots$

x_j is $\dots$

$GCD(|x_i - x_j|, 551)$ is $\dots$

(The GCD should be a factor of 551).

GOTO NEXT PAGE

3. (30 points) Write down TWO facts you learned in the guest lecture on cheating in bridge that you found interesting, and why.

GOTO NEXT PAGE

4. (30 points) Write down TWO facts you learned in the guest lecture on censorship that you found interesting, and why.