1. (0 points) What is the day and time of the timed part of the midterm?
2. (40 points) In this problem you will use the ideas behind Pollard’s \( \rho \)-algorithm to factor 143, 371, and 551.

(a) (15 points) Let \( f(x) = x^2 + 1 \) (mod 143). Let \( x_0 = 7 \).

Compute

\[
x_1 = f(x_0), \quad x_2 = f(f(x_0)), \ldots \text{ until you have two numbers } x_i \text{ and } x_j \text{ who’s difference } |x_i - x_j| \text{ is NOT relatively prime to 143.}
\]

Write down:

\( i \) is . . .

\( j \) is . . .

\( x_i \) is . . .

\( x_j \) is . . .

\( \text{GCD}(|x_i - x_j|, 143) \) is . . .

(The GCD should be a factor of 143).
(b) (10 points) Let \( f(x) = x^2 + 1 \) (mod 371). Let \( x_0 = 7 \). Compute 
\[ x_1 = f(x_0), \quad x_2 = f(f(x_0)), \ldots \] until you have two numbers \( x_i \) and \( x_j \) who’s difference \(|x_i - x_j|\) is NOT relatively prime to 371.

Write down:

\( i \) is \ldots

\( j \) is \ldots

\( x_i \) is \ldots

\( x_j \) is \ldots

\( GCD(|x_i - x_j|, 371) \) is \ldots

(The GCD should be a factor of 371).
(c) (15 points) Let $f(x) = x^2 + 1 \pmod{551}$. Let $x_0 = 7$. Compute
\[ x_1 = f(x_0), \ x_2 = f(f(x_0)), \ldots \] 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 ...
- $j$ is ...
- $x_i$ is ...
- $x_j$ is ...
- $\text{GCD}(|x_i - x_j|, 551)$ is ...

(The GCD should be a factor of 551).
3. (30 points) Write down TWO facts you learned in the guest lecture on cheating in bridge that you found interesting, and why.
4. (30 points) Write down TWO facts you learned in the guest lecture on censorship that you found interesting, and why.