## 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?

   **SOLUTION**

   Oct 28 at 8:00PM

   **END OF SOLUTION**

**GOTO NEXT PAGE**

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

   Compute

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

   Write down:

   $i$ is ...

   $j$ is ...

   $x_i$ is ...

   $x_j$ is ...

   $GCD(|x_i - x_j|, 143)$ is ...

   (The GCD should be a factor of 143).

   **SOLUTION**

   Solution 143: $x_0 = 7$, $x_1 = 50$ so we try $GCD(50 - 7, 143) = GCD(43, 143) = 1$. NO.

   $x_2 = 70$ so we try:
   $GCD(70 - 7, 143) = GCD(63, 143) = 1$ NO, and
   $GCD(70 - 50, 143) = GCD(20, 143) = 1$ NO.

   $x_3 = 39$ so we try:
   $GCD(39 - 7, 143) = GCD(32, 143) = 1$ NO, and
   $GCD(50 - 39, 143) = GCD(11, 143) = 11$. YEAH! 11 is a factor!

   **END OF SOLUTION**

(b) (10 points) Let $f(x) = x^2 + 1 \pmod{371}$. Let $x_0 = 7$. Compute $x_1 = f(x_0)$, $x_2 = f(f(x_0))$, ... 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 ...

$j$ is ...

$x_i$ is ...

$x_j$ is ...

$GCD(|x_i - x_j|, 371)$ is ...

(The GCD should be a factor of 371).

**SOLUTION**

Solution 371:

$x_0 = 7$, $x_1 = 50$ so we try $GCD(50-7, 371) = GCD(43, 371) = 1$. NO.

$x_2 = 275$ so we try

$GCD(275 - 7, 371) = GCD(268, 371) = 1$. NO.

$GCD(275 - 50, 371) = GCD(225, 371) = 1$. NO.

$x_3 = 313$ so we try

$GCD(313 - 7, 371) = GCD(306, 371) = 1$. NO.

$GCD(313 - 50, 371) = GCD(263, 371) = 1$. NO.

$GCD(313 - 275, 371) = GCD(38, 371) = 1$. NO.

$x_4 = 26$ so we try

$GCD(313 - 26, 371) = GCD(287, 371) = 7$. YEAH! 7 is a factor!

$GCD(|x_4 - x_3|, 371) = GCD(313 - 26, 371) = 7$

**END OF SOLUTION**

**GOTO NEXT PAGE**

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

Write down:

$i$ is …

$j$ is …

$x_i$ is …

$x_j$ is …

$GCD(|x_i - x_j|, 551)$ is …

(The GCD should be a factor of 551).

**SOLUTION**

$x_0 = 7$, $x_1 = 50$ so we try $GCD(50-7, 551) = GCD(43, 551) = 1$. NO.

$x_2 = 297$ so we try

$GCD(297-7, 551) = GCD(290, 551) = 29$. YEAH! 29 is a factor!

**END OF SOLUTION**

**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.

   **SOLUTION**

   (These are just mine (Bill's) thoughts. You can and probably did have a different anwser.)

   1) Thinking about a bid can itself give your partner information. This is like a timing attack on RSA!

   2) Cheating in bridge is not punished as harshly as it should be.

   **END OF SOLUTION**

**GOTO NEXT PAGE**

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

**SOLUTION**

(These are just mine (Bill's) thoughts. You can and probably did have a different anwser.)

1) How countries censor is very complicated. Its NOT just looking at every email.

2) There are many ways around censors, but it is a cat-and-mouse game where the censors can read our papers (which give them an advantage) but the breaker-of-censors can always try new things (which gives them the advantage).

**END OF SOLUTION**