# HW 9 CMSC 456. Morally DUE Nov 11
# SOLUTIONS
# NOTE- THE HW IS THREE PAGES LONG

1. (0 points) READ the syllabus- Content and Policy. What is your name? What is the day and time of the FINAL?

   **READ THE MIDTERM SOLUTIONS. EVEN FOR PROBLEMS YOU GOT RIGHT.**

2. (30 points) We want to factor 81072007. We will do a Quadratic Sieve modified so you can do it by hand (also the number is not that large). We outline what you will do AND give you a shortcut!

   - Note that $\lceil\sqrt{81072007}\rceil = 9004$.
   - Normally we would $B$-factor $(9004 + x)^2$ for $0 \le x \le M$. Instead we will factor some of these number entirely.
   - Shortcut: We would like $(9004+x)^2 - 81072007$ to have small factors. Hence we will only pick $x$ such that $(9004+x)^2-81072007 \equiv 0 \pmod 6$.

   An NOW finally for the problem you are to solve:

   (a) (10 points) Fill in the set $X$ in the following sentence. Note that $X \subseteq \{0, 1, 2, 3, 4, 5\}$.
   $((9004 + x)^2 - 81072007 \equiv 0 \pmod 6))$ *IFF* $(x \bmod 6 \in X)$.
   (No proof required.)

   (b) (10 points) For $x \ge 0$ with $x \bmod 6 \in X$, factor $(9004 + x)^2 - 81072007$ until you get what you need for the Quadratic Sieve Algorithm to proceed. (You can use a factor program you find online.)

   (c) (10 points) Use what you got to find a factor of 81072007. You will need to compute a GCD— for this you DO NOT need to show you work. *Very Very Very Good Advice:* When you get what you think is a factor of 81072007, divide 81072007 by the alleged factor to make sure it divides—this will be a good check on your answer.

   **SOLUTION TO PROBLEM TWO**

(a) Fill in the set $X$ in the following sentence. Note that $X \subseteq \{0,1,2,3,4,5\}$.

$((9004+x)^2 - 81072007 \equiv 0 \pmod{6})$ *IFF* $(x \bmod 6 \in X)$.

(No proof required.)

**ANSWER:** We do a proof even though you don't have to.

We want to know what $(9004+x)^2 - 81072007$ is congruent to mod 6.

Since $9004 \equiv 4 \pmod{6}$ and $81072007 \equiv 1 \pmod{6}$ we have

$$(9004+x)^2 - 81072007 \equiv (4+x)^2 - 1 \pmod{6}$$

So we need to know when $(x+4)^2 \equiv 1 \pmod{6}$.

The +4 is, for now, a distraction, so lets see, for which $z$, when $z^2 \equiv 1 \pmod{6}$. We do this by just trying out $z = 0,1,2,3,4,5$.

Only happens when $z \equiv 1,5 \pmod{6}$.

So we need $x+4 \equiv 1,5 \pmod{6}$.

So we need $x \equiv 1,3$

$X = \{1,3\}$

(b) For $x \geq 0$, $x \in X$, factor $(9004+x)^2 - 81072007$ until you get what you need for the Quadratic Sieve Algorithm to proceed.

**ANSWER** All mods are mod 81072007.

| $x$ | $(9004+x)^2$ | $(9004+x)^2 - 81072007$ | | factored |
|---|---|---|---|---|
| 1 | $9005^2$ | $\equiv 18018$ | $=$ | $2 \times 3^2 \times 7 \times 11 \times 13$ |
| 3 | $9007^2$ | $\equiv 54042$ | $=$ | $2 \times 3 \times 9007$ |
| 7 | $9011^2$ | $\equiv 126114$ | $=$ | $2 \times 3 \times 21019$ |
| 9 | $9013^2$ | $\equiv 162162$ | $=$ | $2 \times 3^4 \times 7 \times 11 \times 13$ |

AH-HA! - we can multiply together the first and fourth row

$$(9005 \times 9013)^2 \equiv 2^2 \times 3^6 \times 7^2 \times 11^2 \times 13^2$$

$$(9005 \times 9013)^2 \equiv (2 \times 3^3 \times 7 \times 11 \times 13)^2$$

(c)

$$(9005 \times 9013)^2 \equiv (2 \times 3^3 \times 7 \times 11 \times 13)^2$$

We do the multiplication inside the square, but mod down.

$$90058^2 \equiv 54054^2$$

$$(90058 - 54054)(90058 + 54054) \equiv 0$$

$$36004 \times 144112 \equiv 0$$

So now take

$$GCD(36004, 81072007)$$

It is 9001.
Divide 81072007 by 9001 to get 9007. So

$$81072007 = 9001 \times 9007$$

One can then check that both of these factors are prime.

**GOTO NEXT PAGE**

3. (30 points) Eve wants to factor $G = 139,323,391$ (a product of two primes) using the method Golomb used to factor the Jevons number. This problem will guide you through it. You may use a calculator while doing it, but you must **show your work** as we did on the slides.

   Throughout this problem $x, y$ are such that $G = x^2 - y^2$. During this problem we reduce the number of options for $(x, y)$.

   (a) (6 points) Find a $0 \le d \le 99$ such that the following holds:

   $$y^2 \equiv x^2 + d \pmod{100}$$

   **ANSWER**

   $$G = x^2 - y^2$$

   $$91 \equiv x^2 - y^2 \pmod{100}$$

   $$y^2 \equiv x^2 - 91 \pmod{100}$$

   $$y^2 \equiv x^2 + 9 \pmod{100}$$

   $$d = 9.$$

   (b) (6 points) List all possibilities for $(x^2 \bmod 100, y^2 \bmod 100)$.
   **ANSWER**
   The following is the set of all squares mod 100

   $$\{0, 1, 4, 9, 16, 21, 24, 25, 29, 36, 41, 44, 49\} \cup$$

   $$\{56, 61, 64, 69, 76, 81, 84, 89, 96\}$$

   So we need all pairs that differ by 9 mod 100.

   $$\{(0, 9), (16, 25)\}$$

(c) (6 points) Find all $x \pmod{100}$ such that $x^2 \equiv 0 \pmod{100}$ OR $x^2 \equiv 16 \pmod{100}$. Put the union of the two sets into numeric order. You may use

`https://www.alpertron.com.ar/QUADMOD.HTM`

Note that at the end you will have a small set $A$ such that

$$x \bmod 100 \in A.$$

(Small means size $\le 20$.)

**ANSWER**

$x^2 \equiv 0 \pmod{100}$ has solutions

$$\{0, 10, 20, 30, 40, 50, 60, 70, 80, 90\}$$

$x^2 \equiv 16 \pmod{100}$ has solutions

$$\{4, 46, 54, 96\}$$

Putting it together we get

$$\{0, 4, 10, 20, 30, 40, 46, 50, 54, 60, 70, 80, 90, 96\}$$

(d) (6 points) Show that $x \ge \sqrt{G}$

**ANSWER**

$G = x^2 - y^2$ so

$$x^2 = G + y^2$$

$$x = \sqrt{G + y^2} \ge \sqrt{G}.$$

(e) (6 points) Complete the algorithm and factor $G$.

**ANSWER**

$$x \bmod 100 \in \{0, 4, 10, 20, 30, 40, 46, 50, 54, 60, 70, 80, 90, 96\}$$

$$x \ge \sqrt{G} = 11803$$

$$y = \sqrt{x^2 - 139323391}$$

We now have a table that tries out all $x \geq 11803$

| $x$ | $y = (x^2 - 139323391)^{1/2}$ |
|---|---|
| 11804 | 105 |

WOW- that table ended very fast!
Okay, $x = 11804$, $y = 105$
$x^2 - y^2 = 139323391$
$(x + y)(x - y) = 139323391$

$$(11804 + 105)(11804 - 105) = 139323391$$

$$11909 \times 11699$$

**GOTO NEXT PAGE**

4. (40 points) This is a programming assignment. You will implement Pollard rho's algorithm and use it to find factors of numbers.

   Begin by inputting three lines from standard input. On the first line, an integer $N > 1$ will be given. On the second line, an integer $x$ satisfying $0 \leq x < N$ will be given. On the third line, an integer $c$ satisfying $0 \leq c < N$ will be given.

   Your goal is to use Pollard rho's algorithm (described in the lecture slides) to find a nontrivial factor of $N$ (i.e., a positive factor of $N$ other than 1 and $N$). You will print two lines to standard output. On the first line, you will print out the nontrivial factor the algorithm returns when supplied with the given inputs. Then on the next line, you will print out how many loop iterations the algorithm took before it returned; this value should be on the order of $N^{1/4}$.

   You may assume each test input used by the autograder will not cause Pollard's rho algorithm to get stuck in an infinite loop. So for instance, $N$ will never be prime.

   You may use C, C++, Java, Python2/3, and Ruby for this problem. You will be submitting a zip file containing all code files you used to complete this problem to the Gradescope assignment called
   "hw09 - problem 4".

   Upon submission, your code will be automatically run on a Linux machine and tested against various test cases to ensure correctness. You are allowed to submit your code as many times as you want. As with previous programming assignments, upload a bash script called `run` and (if necessary) another bash script called `build`. These files must begin with the shebang `#!/usr/bin/env bash` on the very first line. If you have any questions or confusions, or if you encounter any technical difficulties, feel free to ask for help on Piazza.