HW On Factoring
SOLUTIONS
NOTE- THE HW IS THREE PAGES LONG

1. (30 points) We want to factor 1488391. 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 $\lceil \sqrt{1488391} \rceil = 1220$.
   - Normally we would B-factor $(1220 + x)^2$ for $0 \le x \le M$. Instead we will factor some of these number entirely.
   - Shortcut: We would like $(1220 + x)^2 - 1488391$ to have small factors. We want the factors 3 and 7 (not sure why we wan that, but we do!). Hence we will only pick x such that $(1220 + x)^2 - 1488391 \equiv 0 \pmod 2)1$.

   An NOW finally for the problem you are to solve:

   (a) (10 points) Fill in the set X in the following sentence. Note that $X \subseteq \{0, \ldots, 20\}$.
   $((1220 + x)^2 - 1488391 \equiv 0 \pmod{21})$ *IFF* (x mod $21 \in X$).
   (No proof required.)

   (b) (10 points) For $x \ge 0$ with x mod $21 \in X$, factor $(1220 + x)^2 - 1488391$ 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 1488391. 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 1488391, divide 1488391 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 $X \subseteq \{0, \ldots, 20\}$.
$((1220 + x)^2 - 1488391 \equiv 0 \pmod{21})$ *IFF* $(x \bmod 21 \in X)$.
(No proof required.)

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

We want to know what $(1220+x)^2 - 1488391$ is congruent to mod 21.

Since $1220 \equiv 2 \pmod{21}$ and $1488391 \equiv 16 \pmod{21}$ we have

$$(1220 + x)^2 - 1488391 \equiv (2 + x)^2 - 16 \pmod{21}$$

So we need to know when $(x + 2)^2 \equiv 16 \pmod{21}$.

The +2 is, for now, a distraction, so lets see, for which z, when $z^2 \equiv 16 \pmod{21}$. We do this by just trying out $z = 0, \ldots 20$.

$$z^2 \equiv 16 \pmod{21}$$

$$z^2 - 16 \equiv 0 \pmod{21}$$

$$(z + 4)(z - 4) \equiv 0 \pmod{21}$$

$z \equiv 4$ or $z \equiv -4 \equiv 17$ but thats not all.

It is possible that $(z+4)(z-4) \equiv 0 \pmod{21}$ with $z+4 \not\equiv 0$ and $z - 4 \not\equiv 0$. We need to have that one of the factors has a 3 and the other has a 7. Trial and error leads to

$z \equiv 10$ or $z \equiv 11$ and

So the set of all z such that $z^2 \equiv 0$ is $\{4, 10, 11, 17\}$

$$X = \{2, 8, 9, 15\}$$

.

(b) For $x \geq 0$, $x \in X$, factor $(1220+x)^2 - 1488391$ until you get what you need for the Quadratic Sieve Algorithm to proceed.

ANSWER All mods are mod 1488391.

x	$(1220+x)^2$	$(1220+x)^2 - 1488391$	factored
2	1222^2	$\equiv 4893$	$= 3\times 7\times 233$
8	1230^2	$\equiv 19593$	$= 3^2\times 7\times 311$
9	1229^2	$\equiv 22050$	$= 2\times 3^2\times 5^2\times 7^2$
15	1235^2	$\equiv 36834$	$= 2\times 3\times 7\times 877$
23	1243^2	$\equiv 56658$	$= 2\times 3\times 7\times 19\times 71$
29	1249^2	$\equiv 71610$	$= 2\times 3\times 5\times 7\times 11\times 31$
30	1250^2	$\equiv 74109$	$= 3\times 7\times 3529$
37	1257^2	$\equiv 91658$	$= 2\times 7\times 6547$
44	1264^2	$\equiv 109305$	$= 3^2\times \times 5\times 7\times 347$
50	1270^2	$\equiv 124509$	$= 3\times 7^3\times 11^2$
51	1271^2	$\equiv 127050$	$= 2\times 3\times 5^2\times 7\times 11^2$

AH-HA- the factorizations of 1229^2, 1270^2, 1271^2 work!
$1229^2 \equiv 2\times 3^2\times 5^2\times 7^2 \pmod{1488391}$
$1270^2 \equiv 3\times 7^3\times 11^2 \pmod{1488391}$
$1271^2 \equiv 2\times 3\times 5^2\times 7\times 11^2 \pmod{1488391}$

$$(1229\times 1270\times 1271)^2 \equiv 2^2\times 3^4\times 5^4\times 7^6\times 11^4$$

$$(1229\times 1270\times 1271)^2 \equiv (2\times 3^2\times 5^2\times 7^3\times 11^2)^2$$

$$1278118^2 \equiv 815658^2 \pmod{1488391}$$

$$(1278118 - 815658)(1278118 + 815658) \equiv 0 \pmod{1488391}$$

$$462460 \times 2093776 \equiv 0 \pmod{1488391}$$

$GD(462460, 1488391) = 1217$ So we get a factor!
One can and should check that 1217 is indeed a factor.

GOTO NEXT PAGE

2. (30 points) Eve wants to factor $G = 1,488,391$ (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 ≤ 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

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

$$x \ge \sqrt{G} = 1219$$

$$y = \sqrt{x^2 - 1488391}$$

We now have a table that tries out all $x \geq 1219$ such that

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

x	$y = (x^2 - 1488391)^{1/2}$
1220	3

WOW- that table ended very fast!
Okay, $x = 1220$, $y = 3$
$x^2 - y^2 = 1488391$
$(x + y)(x - y) = 1488391$

$$(1220 + 3)(1220 - 3) = 1488391$$

$$1223 \times 1217$$

GOTO NEXT PAGE

3. (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.