HW 10 CMSC 456. Morally DUE Nov 18
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 MIDTERM SOLUTIONS

2. (30 points) We want to factor 91. We will do a QS modified so you can do it by hand (also the number is not that large). We are curious for which B this will work. Note that $\lceil \sqrt{91} \rceil = 10$.

   (a) (10 points) In this problem we use $B = 1$ (so can only use the prime 2). Compute and try to 1-factor:
   $(10+0)^2 \pmod{91}$
   $(10+1)^2 \pmod{91}$
   $\vdots$
   until you get a set of 1-fact numbers whose product is a square. Then use that information to factor 91. ALSO- note how many numbers are in the above list (that is, the $(10+i)^2 \pmod{91}$'s). SHOW work, for example the first line is
   $(10+0)^2 = 100 \equiv 9$ NOT 1-fact.

   (b) (10 points) In this problem we use $B = 2$ (so can only use the primes 2,3). Compute and try to 2-factor:
   $(10+0)^2 \pmod{91}$
   $(10+1)^2 \pmod{91}$
   $\vdots$
   until you get a set of 2-fact numbers whose product is a square. Then use that information to factor 91. ALSO- note how many numbers are in the above list (that is, the $(10+i)^2 \pmod{91}$'s). SHOW work.

   (c) (10 points) Recall that the trivial algorithm is to just divide $2, 3, 4, \ldots, \left\lfloor \sqrt{N} \right\rfloor$ into N until one works. How many divisions would this take? Is it more or less time then QS with $B = 1$? $B = 2$? (We count time on the quad sieve, for this problem, as just the length of the list.)

SOLUTION TO PROBLEM TWO

(a) In this problem we use $B = 1$ (so can only use the prime 2). Compute and try to 1-factor:

$(10+0)^2 \pmod{91}$

$(10+1)^2 \pmod{91}$

$\vdots$

until you get a set of 1-fact numbers whose product is a square. Then use that information to factor 91. ALSO- note how many numbers are in the above list (that is, the $(10+i)^2 \pmod{91}$'s).

ANSWER

$(10+0)^2 = 100 \equiv 9$ NOT 1-fact.

$(10+1)^2 = 121 \equiv 30 = 2 \times 15$ NOT 1-fact.

$(10+2)^2 = 144 \equiv 53$ NOT 1-fact.

$(10+3)^2 = 169 \equiv 78 = 2 \times 39$ NOT 1-fact.

$(10+4)^2 = 196 \equiv 14 = 2 \times 7$ NOT 1-fact.

$(10+5)^2 = 225 \equiv 43$ NOT 1-fact.

$(10+6)^2 = 256 \equiv 74 = 2 \times 37$ NOT 1-fact.

$(10+7)^2 = 289 \equiv 16 = 2^4 = 4^2$ YES! 1-fact.

And even better, it's a square.

$$17^2 - 4^2 \equiv 0 \pmod{91}$$

$$(17-4)(17+4) \equiv 0 \pmod{91}$$

$$13 \times 21 \equiv 0 \pmod{91}$$

$GCD(13, 91) = 13$, So 13 is a factor.

Could have also done $GCD(21, 91) = 7$ is a factor.

The list was 8 long.

(b) In this problem we use $B = 2$ (so can only use the primes 2,3). Compute and try to 2-factor:

$(10+0)^2 \pmod{91}$

$(10+1)^2 \pmod{91}$

$\vdots$

until you a set of 2-fact numbers whose product is a square. Then use that information to factor 91. ALSO- note how many numbers are in the above list (that is, the $(10+i)^2 \pmod{91}$'s)

ANSWER

$(10+0)^2 \equiv 100 \equiv 9 = 3^2 \pmod{91}$.

OH, we already have a B-factored number and it is a square.

$$100 - 9 \equiv 0 \pmod{91}$$

$$10^2 - 3^2 \equiv 0 \pmod{91}$$

$$(10-3)(10+3) \equiv 0 \pmod{91}$$

$$7 \times 13 \equiv 0 \pmod{91}$$

$GCD(7, 91) = 7$, so 7 is a factor.

Could also have done $GCD(13, 91) = 13$ is a factor.

The list was 1 long.

(c) Recall that the trivial algorithm is to just divide $2, 3, 4, \ldots, \left\lfloor \sqrt{N} \right\rfloor$ into N until one works. How many divisions would this take? Is it more or less time then QS with $B = 1$? $B = 2$? (We count time on the quad sieve, for this problem, as just the length of the list.)

ANSWER

$B = 1$ took 8 steps

$B = 2$ took 1 step

Trivial takes a step for 2,3,4,5,6,7, so 6 steps.

Trivial is better than $B = 1$ but not as good as $B = 2$.

END OF SOLUTION TO PROBLEM TWO

GOTO NEXT PAGE

3. (30 points) We are going to use the log-trick to detect ahead of time if a number is probably B-fact. We will use $\log_{10}$. We look at the attempt to factor $N = 53044897$ via QS. Note $\left\lceil \sqrt{N} \right\rceil = 7284$. We will use $B = 14$ so the primes are $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43$.

   Below we have many of the first 20 numbers you will come across while trying to do the QS ($\equiv$ is mod N.) We also tell you which of the first 14 primes divides the number.

   (a) For each number y you will do the following.

      i. Compute $\lceil \log_{10}(y) \rceil - \sum_{p \text{ div } y} \lceil \log_{10}(p) \rceil$.
      You may assume that, for all z, $\lceil \log_{10}(z) \rceil$ is the number of digits in z. (Sum is over first 14 primes that divide y.)

      ii. Try to B-factor y and note if it is B-fact.

   (b) Find a number s such that, for all numbers y on the list,

      - y is B-fact implies $\lceil \log_{10}(y) \rceil - \sum_{p \text{ div } y} \lceil \log_{10}(p) \rceil \leq s$.
      - y is not B-fact implies $\lceil \log_{10}(y) \rceil - \sum_{p \text{ div } y} \lceil \log_{10}(p) \rceil \geq s+1$.

   We now present the list with a caveat: we omitted all of them that had either 0 or 1 prime factor within the first 14 primes.

   - $(7284+1)^2 \equiv 26328$. primes that divide this number: 2,3.
   - $(7284+4)^2 \equiv 70047$. primes that divide this number: 3, 43.
   - $(7284+5)^2 \equiv 84624$. primes that divide this number: 2,3,41,43.
   - $(7284+7)^2 \equiv 113784$. primes that divide this number: 2,3,11.
   - $(7284+8)^2 \equiv 128367$. primes that divide this number: 3,17.
   - $(7284+10)^2 \equiv 157539$. primes that divide this number: 3,17.
   - $(7284+11)^2 \equiv 172128$. primes that divide this number: 2,3,11.
   - $(7284+13)^2 \equiv 201312$. primes that divide this number: 2,3.
   - $(7284+17)^2 \equiv 259704$. primes that divide this number: 2,3.
   - $(7284+19)^2 \equiv 288912$. primes that divide this number: 2,3,13.

   ANSWER

- $(7284+1)^2 \equiv 26328$. primes: 2, 3. Diff: $5-1-1=3$.
  $(7284+1)^2 \equiv 26328 = 2^3 \times 3 \times 1097$. NOT B-fact.
- $(7284+4)^2 \equiv 70047$. primes: 3, 43. Diff: $5-1-2=2$.
  $(7284+4)^2 \equiv 70047 = 3^2 \times 43 \times 181$. NOT B-fact.
- $(7284+5)^2 \equiv 84624$. primes: 2,3,41,43. Diff: $5-1-1-2-2=-1$.
  $(7284+5)^2 \equiv 84624 = 2^4 \times 3 \times 41 \times 43$. IS B-fact.
- $(7284+7)^2 \equiv 113784$. primes: 2,3,11. Diff: $6-1-1-2=2$.
  $(7284+7)^2 \equiv 113784 = 2^3 \times 3 \times 11 \times 431$. NOT B-fact.
- $(7284+8)^2 \equiv 128367$. primes: 3,17. Diff: $6-1-2=3$.
  $(7284+8)^2 \equiv 128367 = 3^2 \times 17 \times 839$. NOT B-fact
- $(7284+10)^2 \equiv 157539$. primes: 3,17. Diff: $6-1-2=3$.
  $(7284+10)^2 \equiv 157539 = 3 \times 17 \times 3089$. NOT B-fact
- $(7284+11)^2 \equiv 172128$. primes: 2,3,11. Diff: $6-1-1-2=2$.
  $(7284+11)^2 \equiv 172128 = 2^5 \times 3 \times 11 \times 163$. NOT B-fact
- $(7284+13)^2 \equiv 201312$. primes: 2,3. Diff: $6-1-1=4$.
  $(7284+13)^2 \equiv 201312 = 2^5 \times 3^3 \times 233$. NOT B-fact
- $(7284+17)^2 \equiv 259704$. primes: 2,3. Diff: $6-1-1=4$.
  $(7284+17)^2 \equiv 259704 = 2^3 \times 3^2 \times 3607$. NOT B-fact
- $(7284+19)^2 \equiv 288912$. primes: 2,3,13. Diff: $6-1-1-2=2$.
  $(7284+19)^2 \equiv 288912 = 2^4 \times 3 \times 13 \times 463$. NOT B-fact

We can take $s=-1$. $s=0$ and $s=1$ also work and are probably better.

GOTO NEXT PAGE

4. (40 points) This is a programming assignment. You will write a program that counts the number of B-fact numbers in a given range.

   Begin by inputting three lines from standard input. On the first line, a positive integer B will be given. On the second line, a positive integer x will be given, and on the third line, a positive integer y will be given. You can assume $x < y$. You will print only one value to standard output, namely the number of B-fact numbers in the closed interval $[x, y]$. How you choose to compute this number is entirely up to you.

   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

   "hw10 - 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.

   (a) (30 points) Submit your code files to Gradescope as described above to be tested by the autograder.

   (b) (10 points) Using the program you wrote, create a scatter plot displaying the number of B-fact numbers in the range 1 to 10^5, where B takes on all integers in the range 1 to 100. Submit the plot with the rest of your homework.