

CS 355, Fall, 2019, Project 4

Write a program in Java to find the square roots of a quadratic residue modulo the product of two Blum primes. This is part of the Oblivious transfer protocol. Review the slides in

www.cs.purdue.edu/homes/ssw/cs355/week5.pdf

where you will find all the needed formulas.

The input to your program will be two Blum primes p, q , one per line of standard input, and an integer x between 1 and $pq - 1$ on the third input line. You may assume the first two numbers really are Blum primes and need not check this fact. Assume the primes are $< 10^{100}$ and that $0 < x < pq$. Use the Java BigInteger class to compute with large integers. (The modPow method might be useful.)

Your program will compute $r = x^2 \bmod n$, where $n = pq$. Of course r is a quadratic residue modulo n . You already know two of its four square roots modulo n : x and $n - x$. Your job is to find the other two square roots of r .

Your program should write the other two square roots of r modulo n to standard out, with the smaller one first, and with a single newline after each.

Example:

This is the example solved in the slides. If the input to your program is:

7

19

12

then ($r = 11$ and) your program should write:

26

107

exactly as shown because Vocareum grades by comparing character strings. (Each line ends with a newline character.)

Example:

If the input to your program is:

431

9719

123456

then your program should write:

1412146

2776743

exactly as shown because Vocareum grades by comparing character strings.

Example:

If the input to your program is:

4375578271

2349023

399401322419426

then your program should write:

3857652735639089

6420681261240144

exactly as shown because Vocareum grades by comparing character strings.

Example:

If the input to your program is:

29257554834707791

3156148413859611691

3638898097091030205449202125429103

then your program should write:

41234119542317953998226778601619381

51107065742655654071147294110765200

exactly as shown because Vocareum grades by comparing character strings.

Name your program `sqrt34.java`. Submit your program to Vocareum by 11:59 PM on the due date. It will be compiled and run ten times with ten different secret input sets, each worth 10 points.