

Computational Number Theory

Programming HW 3

Due Date: 28/09/2025

Implement the Tonelli-Shanks algorithm (section 4.7 of notes) for the following:

Input: The input is a csv file with each line having a pair a, p (separated by commas) with p prime and $0 < a < p$, see the sample input file. The number of test cases will be at most 100; each prime will be at most 10 digits long. A sample input file is attached.

Output: For each pair (a, p) , print the smallest positive integer x such that $x^2 \equiv a \pmod{p}$, if it exists, and print -1 otherwise. Print each output on a new line to the standard output (screen).

Output for the given sample input file (inputSquareRoots.csv):

```
16
78
-1
502
456
-1
212022
2352359
84561442
134304
```