Problem 2.17

1137 = 21 (mod 71)

CORRECT

15659 = 116 (mod 593)

CORRECT

650319 = 2213 (mod 3571)

CORRECT

The program created for this question solves the discrete logarithm problem by utilizing Shanks’ baby-step giant-step algorithm and Fermat’s little theorem. The program always outputs a correct answer, and a set of inputs that would print an incorrect solution was unable to be found. The program was written in Python which can handle very large numbers, so there will be no issues with large numbers being rounded incorrectly.