Inverting Modulo

Parker McKillop, Oksana Pooley, Arsh Singh

We implemented a function using the Extended Euclid's Algorithm to find the inverse of a modulo function using extended Euclidean Algorithm. The function can be accessed via this web app. It app produces all the works for a user provided problem.

The definition of multiplicative inverse of A mod B, for two positive integers A and B, is not very far from the definition of multiplicative inverse of an integer. It is an integer x such that when we multiply x and A mod B we get 1.

$$Ax \bmod B = 1$$

For a detailed description of the topic, please see Seymour Lipschutz and Marc L Lipson (2022):

“Properties of the Integers”. In: Schaum’s Outline of Discrete Mathematics. 4th ed. Accessed via Northeastern University Library. New York: McGraw Hill, 2022. Chap. 11. url: https://www.accessengineeringlibrary.com.ezproxy.neu.edu/content/book/9781264258802/chapter/chapter11