Explaining the Map and the Matrix of the Discrete Lambert Exponentiation

Kumar, Krishan

Given a number x, we consider the dynamic system x goes to x(g^x) mod (p^n), also known as the Discrete Lambert. In this equation, all variables are known other than x. The Discrete Lambert has puzzled mathematicians around the world for decades. The reason x is so difficult to solve for is that the variable p, which is a prime number, may be hundreds of digits long, meaning that even with the assistance of computer technology, it may take over a hundred years to solve. In the context of this research, smaller examples were used so that proofs could then be drawn on a much larger scale. To visualize this cycle an accompanying map, which illustrates each number and what number it results in when plugged into the original equation, and matrix may be illustrated. In this research an algorithm is extracted which is able to allow any such map to be drawn with accuracy without having to plug in every number x into the generator g until a pattern is identified. When the map is actually drawn out, certain numbers, x, will form sets and each element of that set will only go to another element of that set when plugged into the function. By noticing a pattern in the arrangement of numbers in these groups and patterns in the relating matrices, proofs were deciphered and theorems were distinguished. The Discrete Lambert problem relates to other functions such as the Discrete Logarithm and encryptions known as digital signatures. They are used to verify the authenticity of legal documents, financial transactions, and other important communications. It is evident that these encryptions are a key element to our society and can impact major domestic and even international transactions. This research will have further implications and successfully maps part of the Discrete Lambert.

Awards Won:
Fourth Award of $500