THE UNIVERSITY OF CHICAGO | DEPARTMENT OF STATISTICS

MASTER'S THESIS PRESENTATION

XIAOYU LEI

Department of Statistics
The University of Chicago

How To Get A Discrete Uniform Distribution From A Biased Coin?

—An application of random variable in residual classes

FRIDAY, October 14, 2022, at 4:30 PM
Jones 226, 5747 S. Ellis Avenue

ABSTRACT

The residual classes Z/nZ, as an algebraic system different from the integers Z, has its unique arithmetical features. Although it is an important subject of study in algebra, it is hardly connected with probability theory. In this talk, I will introduce the random variables taking values in residual classes. Then we will see how this idea helps us prove the validity of a random number generation algorithm.

In this talk, we will first consider a classic problem: how do we get a discrete uniform distribution given a biased coin? I will propose a novel algorithm, which improves the efficiency of the previous algorithm. Then I will introduce the modulo function and residual classes. The well-definedness of addition and multiplication on the residual classes will be shown, and we will see the arithmetical features of residual classes Z/nZ, especially when n is prime. We will see any nonzero element in Z/pZ can generate Z/pZ for prime p. Next I will introduce the random variables taking values in the residual classes. The distribution of random variable and the independency will also be introduced by analogy with the definitions in probability theory. Finally, I will prove the validity of the algorithm proposed above using random variables in residual classes. The proof combines the probabilistic analysis with algebraic techniques, inspired by the unique arithmetical structure of Z/pZ . Both the algorithm and its proof are interesting and innovative.