Preface

The Monte Carlo method is a numerical method to solve mathematical problems by computer-aided sampling of random variables. It has started when von Neumann, Ulam and others applied it to the simulation of nuclear fissions[†1] by newly invented computers in 1940's, i.e., in the midst of World War II ([16]). Since then, along with the development of computer, the Monte Carlo method has been used in all fields of science and technology, and has produced remarkable results. The development of the Monte Carlo method will surely continue.

In this monograph, however, we do not deal with such brilliant applications of the method, but we mainly discuss its mathematical foundation, in particular, the justifiability of computer-aided sampling methods. That is, there is a fundamental difficulty that computers cannot generate random numbers, so that we use pseudorandom numbers instead of them in Monte Carlo methods. Here, a number of researchers have had a serious suspicion;

> *Monte Carlo methods using pseudorandom numbers can never have any mathematical justification.*

As a matter of fact, this suspicion is merely a misunderstanding due to the prejudice caused by intuitive interpretations of the Monte Carlo method, random number and pseudorandom number.[†2] Namely, learning the notions of random number and pseudorandom number correctly, and formulating the Monte Carlo method properly, we see that there is the possibility to remove this suspicion, and in fact, that we can actually remove it in many cases. In this monograph, we give detailed explanations about this. At the same time, the reader will find that such a proper mathematical formulation of the Monte Carlo method leads to the development of the most reliable computer-aided sampling methods.

How to execute sampling of random variables by computer has been an important issue since the Monte Carlo method came into the world. In 1960's, Kolmogorov and others defined the notion of random number by using a function which is called "the Kolmogorov complexity" today ([5, 18, 19, 20, 26]). It was an epoch-making work that was done by making free use of the theory of computation, which theory was initiated in 1930's. About 20 years after their works, in 1980's, Blum and others defined the notion of pseudorandom number in the context of cryptography ([2, 3, 49]). It was based on the

[†1] In order to make atomic bombs.

[†2] Many references about the Monte Carlo method do not distinguish random number and pseudorandom number. For instance, although the chapter title of [17] is "Random numbers", it actually deals with pseudorandom number. In this monograph, they are strictly distinguished.