

Abstract

An integer Z101 is divided by an integer I102 to obtain a remainder R109. The integer I102 includes a polynomial of power of a basic operational unit of a computer. In this way, the integer I for divisor is limited based on the basic operational unit of the computer, thus a shift operation, which is required for a conventional operation method, can be eliminated. The remainder can be calculated by only addition and subtraction. Accordingly, a code size becomes compact and the remainder of the integer can be calculated at a high speed.