Chaos and Correlation
International Journal, March 7, 2016

АЛГОРИТМ ИЗВЛЕЧЕНИЯ КОРНЯ НЕЧЕТНОЙ СТЕПЕНИ В НАТУРАЛЬНЫХ ЧИСЛАХ: ПУТЬ СПРАВА НАЛЕВО

В. Я. Розенблат, Б. В. Розенблат

Излагается новый алгоритм извлечения натурального корня n-ной степени в B-ичной системе счисления, где B свободно от квадратов, а n нечётно и взаимно просто с $p - 1$ для всех простых делителей p числа B. В частности, для любого нечетного n алгоритм применим к произвольному натуральному S, записанному в системах счисления с основанием $2, 3, 5$ или 10. Предлагаемый алгоритм обрабатывает «справа налево» заданную на входе B-ичную запись числа S и вычисляет натуральный корень n-ной степени из S, если он существует. Если корня нет, то вычисляется наименьшее натуральное x, дающее совпадение "правого хвоста" B-ичной записи n-ной степени числа x с числом S по всей длине S, если есть такое x. Если же указанного x нет, то выдаётся сообщение об отсутствии натурального корня из-за «несовместимости» в соответствующем разряде B-ичной записи S. Результаты работы могут быть полезными при решении двучленных сравнений высокой степени, а также могут использоваться в криптографии.

Ключевые слова: алгоритм извлечения натурального корня нечётной степени «справа налево».

n-TH ROOT ALGORITHM IN INTEGERS FOR ODD n : A WAY FROM RIGHT TO LEFT

V. Ya. Rozenblat, B. V. Rozenblat

Let B be the base of the number system to be used, and n be the degree of the root to be extracted. A new n-th root algorithm in integers is given for the case when B is square-free, n is odd and n has no common divisors with $p - 1$ for any prime divisor p of B. In particular, for any odd n , one can use this algorithm for any integer S, presented in the number system with the base $2, 3, 5$ or 10. The algorithm gets the B-presentation of S as input, works with it "from right to left" and calculates the integer n-th root from S if it exists. If there is no such root, the algorithm calculates the least integer x such that the "right tail" of the B-presentation of the n-th degree of x coincides with S, if there exists such x. If there is no such x, the message is produced about non-existence of the integer n-th root caused by "non-consistency" in the correspondent digit of the B-presentation of S. The results of the present work can be useful in solving two-member congruences of high degree; they can be also used in cryptanalysis.

Keywords: n-th root algorithm in integers for odd n, which works "from right to left".

18 страниц на русском языке: http://chaosandcorrelation.org/Chaos/RR1_7_3_2016.pdf