A New Rule on Divisibility by (c - 1) * c^k and Its Application in Cryptology

Cevik, Ibrahim Muhammed (School: Tofas Fen Lisesi)

Divisibility rules which are used to detect divisibility of numbers are memorable and practical rules and methods which are different for each number. A new study has been conducted to improve these rules and to find a new divisibility rule and a common divisibility rule for the numbers 15 and 18 has been observed. According to the study on this common divisibility rule, this happens because they are divisors of 90. After that, it has been studied to develop this common rule and it has been improved for 9×10k and its divisors. It has been proved for all the induction divisors of 9×10k through the direct proof method. Then it has been thought that this rule is valid modulo (c − 1) × ck and it has been generalized to its divisors. A study has been conducted about the use of the improved rule and it has been thought that this divisibility rule can be used in Cryptology as Maths is the base of Cryptology and Modular Arithmetic is widely used in Cryptology. After browsing literature and examining the criteria that have to be found in Cryptology, a basic encryption method that uses this method has been developed. It has been concluded that the new divisibility rule can be used in Cryptology and it was developed to provide the numerical values of letters and characters of the text by using irrational numbers and to encrypt these numerical values by converting them into 3 components by using the divisibility rule.