On a New Variant of Prime Factorization Algorithm

Ooi, Zhi Ping (School: Chung Ling High School Penang)
Tee, Jin Xian (School: Chung Ling High School Penang)

For centuries, prime factorization has been a fundamental theoretical problem in the mathematical world. Conventionally, the algorithms for prime number factorization demand a computational cost that grows exponentially with the magnitude of number to be factorized. Existing algorithms will hit a formidable barrier due to the finite computation resource practically available. In this research, we have attempted to introduce a new and effective approach: an improvement of Fermat's Factorization algorithm. Our method mainly involves two variables k and s, s = ceil(sqrt(n*k)), where k is a natural number. This ensures that in most of the cases, we get a small value from s^2 mod n, which aids in finding factors as the distribution of perfect squares are denser at smaller numbers. Results have shown that our approach is capable of prime factorizing numbers hundreds of times faster than the original method, Fermat's Factorization algorithm, while being almost on par with Pollard's Rho. For all of the numbers aside of certain semiprimes, our algorithm can factorize it under <0.01 second. Besides, our new method allows us to implement parallel processing while searching for factors, greatly increasing its efficiency. Therefore, this approach is a new gateway to creating an efficient prime factorizing algorithm, hence bringing benefits to the mathematical field.