An Elementary Method for Fast Modular Exponentiation With Factored Modulus

Aggarwal, Anay (School: Jesuit High School)
Isaacs, Manu (School: Jesuit High School)

The rise of modern cryptosystems introduced the problem of modular exponentiation. Modular exponentiation is the problem of computing a perfect power a^n modulo some modulus, say m. This problem is remarkably useful because its inverse problem, the discrete logarithm problem, is computationally hard. This makes for systems that are difficult to hack. We discover a fast algorithm for modular exponentiation in the case where the prime factorization of the modulus is known. We show that, in general, our algorithm performs asymptotically better than the current fastest algorithm (by certain metrics). While this is true, we pay particular attention to the case where the exponents in the prime factorization of the modulus are large. For this case, we achieve a complexity on the order of the square root of the complexity of current algorithms. We prove our theoretical results empirically by comparing ourselves to Python's optimized pow function. The ideas used in our algorithm have significant general consequences; they produce analogous results for matrices and even more general algebraic structures. We hence improve Fiduccia's algorithm for computing large terms of linear recurrent sequences. Our algorithm has huge potential for applications in cryptography and coding theory. We open up a new study of cryptosystems that use a modulus with large prime factors, providing fast encryption and decryption for such systems. Additionally, a current area of research is using matrix modular exponentiation and linear recurrent sequences for error-correcting codes. Our work can hence potentially provide fast encoding algorithms.