A Solution of Generalized Legendre's Equation Cz^n=Ax^2+By^2 and Its Application to Cryptography

Suprun, Yuliia (School: Municipal Institution Sumy Specialized School of I-III Levels Named After the Hero of the Soviet Union O. Butko)

The Diophantine equation Ax^2+By^2+Cz^2=0 is named for Adrien-Marie Legendre, who found in 1785 a necessary and sufficient condition for the existence of non-trivial integer solutions to this equation. At the moment the main approach to solve this equation is to find some small solutions and using recurrent formulas get a series of primitive solutions for each small solution. Works of Holzer, Mordell, Williams, Cochrane, Mitchell are dedicated to this approach. The purpose of this research is the analysis of the Diophantine equation Cz^n=Ax^2+By^2, where n is any natural number, which could be considered the generalized Legendre's equation. During this research, I used methods of the number theory and information technology. New necessary and sufficient conditions were established for the existence of non-trivial integer solutions of generalized Legendre's equation. Relations between the coefficients of equation allow obtaining new formulas of solutions without a recurrent approach. Using the obtained results, I built the algorithm for solving the Diophantine equations of this type: Cz^n=Ax^2+By^2, where n is any natural number. To verify results, a program was created for finding solutions of the corresponding equation. The obtained results could be used in various areas, e.g. in cryptography – a new key agreement protocol and asymmetric cryptosystem were introduced, which are based on solution finding of generalized Legendre's equation with common parameters.

Awards Won:

National Center Junior Academy of Sciences of Ukraine: UN Sustainable Development Goal Award $ 500.00