In this research, we develop a new integer factorization algorithm which has polynomial running time for certain integers. The algorithm is based on binary quadratic forms of a positive discriminant. A binary quadratic form is an integer valued function \( F(x, y) = ax^2 + bxy + cy^2 \) such that \( \gcd(a, b, c) = 1 \). The discriminant of \( F(x, y) \) is \( \Delta = b^2 - 4ac \).

There is an equivalence relation between binary quadratic forms of the same discriminant. For the set of equivalence classes of binary quadratic forms, Gauss defined a group operation called composition of binary quadratic forms. Groups behave distinctly for negative and positive discriminants. For a negative discriminant, each equivalence class has a unique representative which is called a reduced form. On the other hand, for a positive discriminant each class does not have unique representative of reduced form. However, each reduced form in a class belongs to a unique cycle. We show that for certain kind of integers \( n \) which are especially being used in RSA crypto system, if we start with a reduced form \( (1, b, c) \) of discriminant \( n \) and if we proceed on the cycle, we end up with a form, \( (k_1p, k_2p, d) \) such that \( p \) is a nontrivial divisor of \( n \). (Received September 26, 2017)