Mollin, R. A. (3-CALG)

All solutions of the Diophantine equation \( x^2 - Dy^2 = n. \)

(English. English summary)


In this article the problem considered by the author is that of generating all proper solutions to the quadratic Diophantine equation \( x^2 - Dy^2 = Q, \) for any radicand \( D \) and arbitrary integer \( Q. \) The means is an infrastructure between ideal theory and the continued fraction algorithm (CFA). The problem has a lengthy history [L. E. Dickson, History of the theory of numbers. Vol. II, Chelsea, New York, 1966; MR0245500 (39 #6807b)], and the author presents a complete solution. The paper begins with basic terminology in the theory of quadratics [R. A. Mollin, Quadratics, CRC, Boca Raton, FL, 1996; MR1383823 (97e:11135)]. Several results on ideals are stated, including the ideal criterion for nonzero ideals \( I = [a, b + c\omega], \) where \( \omega \) is the principal surd associated with the discriminant \( \Delta, \) and the criterion for ideal equality pertaining to a primitive ideal \( I = [a, \alpha] \) in \([1, \omega]\), an order in \( \mathbb{Q}(\sqrt{\Delta}). \) The recurrence relations of the CFA for a quadratic irrational \( \gamma \) are stated; they depend on \( D \) and on generated sequences \( P_i, \) \( Q_i \) such that \( Q \mid P^2 - D. \) Moreover, in the CFA a sequence of equivalent ideals is generated. Known results concerning solutions to the equation \( x^2 - Dy^2 = \pm 1 \) are also presented using the CFA. The equation \( x^2 - Dy^2 = Q, \) \( |Q| < \sqrt{D} \) was studied by X. Zhang, in whose work [“Semi-simple continued fractions and Diophantine equations for real quadratic fields”, Internat. Center Theoret. Phys. Preprint IC/94/257, 1994], in an attempt to generalize, was apparently left a conjecture which was solved by the author. A result of Lagrange is stated equating the fundamental unit \( \varepsilon_\Delta \) to the product of \( l \) (period in CFA) quadratic irrationals. Related ideas are used by the author in proving the main theorems, in particular, the fact that \( \varepsilon^m \) can be written as \( \tilde{G}_{m-1} \tilde{B}_{m-1} \sqrt{D}, \) where \( m \) is any positive integer. The tilde notation refers to the periodic continued fraction expansion of

\[ P_n + \sqrt{D} = (\tilde{a}_0; \tilde{a}_1, \ldots, \tilde{a}_{i+1}, \tilde{a}_{i+2}, \ldots, \tilde{a}_{i+l}), \]

for some \( i \geq 0; \) \( \tilde{a}_i \) arises in recurrence relations for \( \tilde{G} \) and \( \tilde{B}, \) \( n \) is the principal reduction index \( (Q_n = 1) \) and \( l \) is the period of the continued fraction expansion of \( P_n + \sqrt{D}. \) The main results include the existence of a unique ideal \( I = [Q_0, P_0 + \sqrt{D}] \) that corresponds to a primitive solution \( \alpha_0 = x_0 + y_0\sqrt{D} \in [1, \sqrt{D}] \) and a unique primitive element.
$\alpha = x + y\sqrt{D}$, where $\alpha_0\alpha' = P_0 + \sqrt{D}$ and $N(\alpha_0) = Q_0$ ($N$ is the norm and prime means conjugate). Another result gives the positive and negative associates (positive if $\beta = \varepsilon_i\Delta\alpha$ and $i > 0$, negative if $i < 0$) of the fundamental, proper solution $\alpha_0$, the former given by $\delta_k(m) = G_{k(m)} + B_{k(m)}\sqrt{D} \neq \alpha_0$, where $m$ is an arbitrary nonnegative integer and $k(m) = lm + n - 1$ is odd. The latter has a slightly different form, namely, $\delta_k(m) = -\tilde{G}_{k(m)} + \tilde{B}_{k(m)}\sqrt{D}$, where the double dot notation corresponds to $-\alpha'_{0}$. The main theorem extends the previous result to yield all positive [negative] associates such that $m > m_0$ [resp. $\tilde{m}_0$] where $m_0$ is the least non-negative integer such that $k(m_0)$ is odd, and specifies $\alpha_0$ in terms of associates depending on $m_0$ or $\tilde{m}_0$. A result shows that given all fundamental proper solutions, all proper solutions are of the form $\pm G_{k(m)} + B_{k(m)}\sqrt{D}$, depending on the negative or positive associates. The author also forms results from the motivating work of Zhang [op. cit.]. A result shows that $G_{k(m)} = \hat{A}_{k(m)}$ and $B_{k(m)} = -\hat{B}_{k(m)}$, where the hat notation corresponds to the continued fraction expansion of $\sqrt{D}$. Moreover $G_{k(m)}^2 - B_{k(m)}^2D = Q$ under the same assumptions for $k(m)$, and this is equivalent to $\alpha_0$ being a proper solution. The main result lists other equivalent statements to $\alpha_0 = x_0 + y_0\sqrt{D}$ being proper, one of which is $x_0/y_0 = \pm G_{k(m)}/B_{k(m)}$ or $x_0/y_0 = \pm \tilde{G}_{k(m)}/\tilde{B}_{k(m)}$ for some $m \geq 0$. In summary, the author has bridged ideal theory with the CFA to establish a complete solution of $x^2 - Dy^2 = Q$. George W. Grossman (1-CMI)