On the Diophantine Equations

\[ ax^2 + bx + c = c_0c_1^{y_1}\cdots c_r^{y_r} \]

Christoph Hering
Mathematisches Institut, Universität Tübingen, Auf der Morgenstelle 10, D-72076 Tübingen, Germany

Received August 28, 1991; revised version November 7, 1994

Abstract. An algorithm is devised to determine all solutions of any Diophantine equation of the type described in the title.

Keywords: Diophantine equations, Cyclotomic polynomials, Perfect codes.

We construct a general algorithm to determine all solutions of Diophantine equations of the form \( ax^2 + bx + c = c_0c_1^{y_1}\cdots c_r^{y_r} \), where \( a, b, c, c_0, \ldots, c_r \in \mathbb{Z} \). The process uses the theory of real quadratic fields. An analysis of Pell's equation \( x^2 - 1 = Dy^2 \) and a specially adapted description of the set of solutions of the equation \( x^2 - m = Dy^2 \) is applied in order to reduce the problem to the following question in Diophantine linear algebra: Let \( M \) be an integral \( 2 \times 2 \)-matrix and \( x, y \in \mathbb{Z} \). How can one determine all images \((x', y') = (x, y)M^i\) where \( i \in \mathbb{N} \) (or \( i \in \mathbb{Z} \), if \( M \) is invertible), such that the prime divisors of \( y' \) belong to a specified set of primes (see Sect. 3)?

As an application of the algorithm we determine all solutions of the equations \( x + 1 = 2^\alpha 5^\beta \) and \( x^2 + x + 1 = 3^\alpha 7^\beta 13^\gamma \). Because these two Diophantine equations are very important for various group theoretical and geometric problems (see e.g. [5]), we present detailed proofs. Actually, the paper was inspired by a more general question on cyclotomic polynomials, namely if it might be possible to determine all \( x \in \mathbb{Z} \) and \( n \in \mathbb{N} \), \( n \geq 3 \), such that no prime divisor of \( \Phi_n(x) \) surpasses \( 2n + 1 \). (Here \( \Phi_n(x) \) is the \( n \)th cyclotomic polynomial.) This is essentially equivalent to determining all solutions of the Diophantine equations

\[ \Phi_n(x) = p^{\alpha'}(n + 1)^{\beta'}(2n + 1)^{\gamma'}, \]

where \( p \) is the largest prime divisor of \( n \). A solution of this problem would be extremely useful for many areas in group theory and geometry. The above results lead to an affirmative answer, if \( n = 2^\alpha 3^\beta \), where \( \alpha \neq 1 \) (see [6]).

Finally, we mention that the algorithm also immediately solves the very interesting Diophantine equation \( x^2 + 7 = 2^\alpha \) of Ramanujan, which was first resolved by Nagell [8] and later investigated by Skolem, Chowla and Lewis [11], Dunton [2],
Browkin and Schinzel [1], Mordell [7], Hasse [3] and others (see Hasse [3]). In fact, our algorithm without great difficulty also determines all solutions of the equation
\[ x^2 + 7 = 2^r \cdot 3^s \cdot 5^t \cdot 7^u \cdot 11^v \cdot 13^w \cdot 17^x \cdot 19^y \cdot 23^z. \]

There are also connections to coding theory. Every perfect two error correcting code leads to a Diophantine equation of the type considered here. Applying our algorithm one obtains extensive information on the possible parameters.

1. A Sieve with Wide Meshes

Let \( a, b, c, c_0, c_1, \ldots, c_r \in \mathbb{Z} \). We want to determine the solutions \((X, Y_1, \ldots, Y_r)\) of the equation
\[ aX^2 + bX + c = c_0c_1^{Y_1} \cdots c_r^{Y_r}, \tag{1} \]
such that \( X \in \mathbb{Z} \) and \( Y_1, \ldots, Y_r \in \mathbb{N} \cup \{0\} \). (Throughout this paper, \( \mathbb{Z} \) denotes the set of rational integers and \( \mathbb{N} \) the set of natural numbers.)

We assume w.l.o.g., that \( r \geq 1 \), \( a \neq 0 \) and \( c_0, c_1, \ldots, c_r \neq 0 \). (For \( a = 0 \), see p. 9, case \( m = 0 \).) Determine \( u, v, k \in \mathbb{Z} \) such that \( k \neq 0 \), \( u^2 = ka \) and \( 2uv = kb \). (For example, choose \( k = 4a \), \( u = 2a \) and \( v = b \) or \( u = k = a \) and \( v = b/2 \) if \( b \) is even. The smallest absolute value of \( k \) is obtained by \( k = 4a/t^2 \), \( u = 2a/t \) and \( v = b/t \), where \( a = a_1^2a_2 \) such that \( a_2 \) is squarefree, and \( t \) is the greatest common divisor of \( 2a_1 \) and \( b \).) Denote \( x = uX + v \) and \( m = v^2 - kc = (k/4a)(b^2 - 4ac) \). Then
\[ x^2 - m = kc_0c_1^{Y_1} \cdots c_r^{Y_r}. \]

For every subset \( X \subseteq \{1, \ldots, r\} \) denote
\[ D(X) = kc_0 \prod_{i \in X} c_i. \]

Choose integers \( d \) and \( D \) such that \( D(X) = D \cdot d^2 \) and consider the Diophantine equation
\[ x^2 - m = Dy^2 = (D(X)/d^2)y^2. \tag{2} \]

It is now clear that the problem to determine all solutions of (1) is equivalent to the problem to determine all solutions \((x, y)\) of one of the Diophantine equations (2) for which \( y = dc_1^{z_1} \cdots c_r^{z_r} \) for suitable non-negative integers \( z_1, \ldots, z_r \) and also \( x \equiv v \pmod{u} \).

2. The Solutions of \( x^2 - m = Dy^2 \)

Let \( m \in \mathbb{Z} \) and \( D \in \mathbb{N} \) such that \( D \) is not a square (so in particular \( D > 1 \)). Let \((\xi, \eta)\) be a positive integral solution of \( x^2 - 1 = Dy^2 \), i.e. \( \xi^2 - 1 = D\eta^2 \) and \( \xi, \eta \in \mathbb{N} \). We define
\[ M = \begin{bmatrix} \xi & \eta \\ D\eta & \xi \end{bmatrix}, \quad I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad J = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \]
and \( G \) to be the group generated by \( M, J \) and \(-I\). Then \( G \) is a group of integral matrices of determinant \(+1\) or \(-1\). As
\[ J^{-1}MJ = \begin{bmatrix} \xi & -\eta \\ -D\eta & \xi \end{bmatrix} = M^{-1}, \]